ELECTION SECURITY

HEARING

BEFORE THE

COMMITTEE ON HOUSE ADMINISTRATION HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MAY 8, 2019

Printed for the use of the Committee on House Administration

Available on the Internet:
https://www.govinfo.gov/committee/house-administration

U.S. GOVERNMENT PUBLISHING OFFICE
38–641 WASHINGTON : 2020

COMMITTEE ON HOUSE ADMINSTRATION

ZOE LOFGREN, California, *Chairperson*

JAMIE RASKIN, Maryland
SUSAN A. DAVIS, California
G. K. BUTTERFIELD, North Carolina
MARCIA L. FUDGE, Ohio
PETE AGUILAR, California

RODNEY DAIVS, Illinois
Ranking Member
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia

CONTENTS

MAY 8, 2019

ELECTION SECURITY

WEDNESDAY, MAY 8, 2019

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOUSE ADMINISTRATION,
Washington, DC.

The Committee met, pursuant to call, at 2:17 p.m., in Room 1310, Longworth House Office Building, Hon. Zoe Lofgren [Chairperson of the Committee] presiding.

Present: Representatives Lofgren, Raskin, Davis of California, Butterfield, Fudge, Davis of Illinois, Walker, and Loudermilk.

Staff Present: Khalil Abboud, Deputy Staff Director; Sean Jones, Legislative Clerk; David Tucker, Parliamentarian; Tanya Sehgal, Senior Elections Counsel; Veleter Mazyck, Chief of Staff to Representative Fudge; Lauren Doney, Communications Director and Deputy Chief of Staff to Representative Raskin; Julie Tagen, Chief of Staff to Representative Raskin; Brandon Mendoza, Senior Legislative Aide to Representative Davis of California; Lisa Sherman, Chief of Staff to Representative Davis of California; Kyle Parker, Senior Policy Advisor to Representative Butterfield; Evan Dorner, Legislative Assistant to Representative Aguilar; Joy Yunji-Lee, Minority Counsel; Courtney Parella, Minority Communications Director; Jesse Roberts, Minority Counsel; Cole Felder, Minority General Counsel; Jen Daulby, Minority Staff Director; and Susannah Johnston, Legislative Assistant to Representative Loudermilk.

The CHAIRPERSON. Good afternoon. The Committee on House Administration will come to order. We do thank the witnesses for being here with us today. This Committee is charged with overseeing the administration of Federal elections, and this hearing will help us fulfill that responsibility by documenting the scope of current election security challenges.

Before we proceed, I offer this background on today's troubling state of affairs. It is documented that foreign agents, specifically Russians, attempted to interfere in American elections in 2016. The fact of Russian interference in the 2016 election was confirmed by eight credible national entities, the Central Intelligence Agency, the Office of Director of National Intelligence, the FBI, the National Security Agency, the Department of Justice, the Department of Homeland Security, and the House Intelligence Committee and the Senate Intelligence Committee.

There was not only consensus among American intelligence officials, both Democrats and Republicans agree that attempts were made by Russia to compromise the integrity of American elections. On July 17, 2018, then House Speaker Paul Ryan said to reporters: They did interfere in our elections; it is really clear.

Senate Majority Leader Mitch McConnell referred to indisputable evidence of Russia's attempt to influence the 2016 election. Senate Majority Leader McConnell further stated: "We understand the Russian threat, and I think that is the widespread view here in the United States among members of both parties."

More details of foreign interference in our election became known through the release of Special Counsel Robert Mueller's report which detailed the following, quote: "GRU officers, the main military foreign intelligence service of Russia, also targeted individuals and entities involved in the administration of the elections." Victims included U.S. State and local entities, such as State boards of election, secretaries of state, and county governments, as well as individuals who worked for those entities. The GRU also targeted private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter regulation software and electronic polling stations.

In June 2017, then Democratic Leader Pelosi created the Congressional Task Force on Election Security in response to then the inaction on the topic. Despite our clear responsibilities under House Rules, not a single hearing was held in this Committee on this topic in the last Congress.

In February 2018, the Task Force released its report, recommending reforms that could significantly advance election security. Among some of the proposed reforms are replacement of paperless voting machines with paper ballot voting systems, risk-limiting audits, upgraded information technology infrastructure, including voter registration databases with ongoing maintenance, and requirements that election technology vendors secure their voting systems.

Intelligence community pre-election threat assessments, in coordination with Federal and State officials is important, and it also prioritized State-level cybersecurity training. Congress has not done enough to tackle this problem. The risk posed by the vulnerabilities previously exploited remain. Despite the overwhelming evidence showing these vulnerabilities, the White House has failed to take these issues seriously and to direct resources towards securing election infrastructure.

Last summer, in remarks before the National Association of the Secretaries of State, former Homeland Security Secretary Kirstjen Nielsen said that there was, quote, "no indication that Russia is targeting the 2018 U.S. midterms at a scale or scope to match their activities in 2016 but that she "consistently observed malicious cyber activity from various actors against U.S. election infrastructure."

She also said that, quote, "there is little doubt that adversaries and non-State actors continue to view elections as a target for cyber and influence operations."

Now, according to *The New York Times*, Homeland Security Secretary Nielsen eventually gave up her efforts to organize a White House meeting of Cabinet Secretaries to coordinate a strategy to protect next year's elections. As a result, the issue did not gain urgency or widespread attention that only a President can command, and it meant that many Americans remained unaware of the latest versions of Russian interference.

In spite of inaction, the Election Assistance Commission, in cooperation with the Department of Homeland Security, has been successful at building relations with State officials and providing valuable resources as part of the critical infrastructure designation. But in the face of increasing threats, their efforts must expand. However, such expansion is only possible if Congress increases resources.

Today, the EAC is operating with only half the budget and fewer than half the staff it had 10 years ago when threats were less grave. This already under resourced agency is only further stymied by the administration's strenuous efforts to avoid acknowledging our vulnerability and the need to secure our elections from foreign threats, facts accepted as plain by both legislative branch and national intelligence agencies. This is unacceptable, and several things must change.

States need money to be able to replace their paperless voting machines and outdated IT infrastructure. States and localities also face the daunting task of training hundreds, if not thousands, of election officials, IT staff, and poll workers on cybersecurity and risk mitigation.

Another significant vulnerability comes from election technology vendors. Many States purchase their voting systems from third-party vendors who have little financial incentive to prioritize election security and are not subject to regulations requiring them to use cybersecurity best practices, nor are they necessarily voluntarily adhering to these best practices.

In July of 2018, it was revealed that ES&S, one of the Nation's largest voting machine makers had installed remote access software on election management systems, although it had not admitted about this fact to the press. This fact was only uncovered through an inquiry by Senator Ron Wyden, who characterized this remote access software installation as, quote, "the worst decision for security, short of leaving ballot boxes on a Moscow street corner."

In addition, election vendors are not currently required to inform any Federal agency or State election official in the event of a cyberattack. Federal action is needed now to grasp the scope of the problem and to innovate concrete solutions that can be implemented before the next Federal election cycle in 2020. This goal will be a primary focus of this Committee moving forward. No matter your side of the aisle, the oath of upholding democracy as citizens and elected leaders in this Nation is fundamental, and that is why I am glad to convene this hearing today, especially recognizing our new Ranking Member Rodney Davis' avowed commitment to advancing election security so that every voter can feel that her vote is accurately counted and safe from the influence of those who wish to see our great democratic experiment fail. And with that goal in mind, I would recognize Mr. Davis for his opening statement.

[The statement of the Chairperson follows:]

Congress of the United States
House of Representatives
COMMITTEE ON HOUSE ADMINISTRATION
1309 Longworth House Office Building
Washington, D.C. 20515–6157
(202) 225–2061
https://cha.house.gov

Chairperson Zoe Lofgren
Hearing on Election Security
May 8, 2019
Opening Statement

Good afternoon. This committee is charged with overseeing the administration of federal elections; this hearing will help us fulfill that responsibility by documenting the scope of current election security challenges.

Before we proceed, I offer this background on today's troubling state of affairs: It is documented that foreign agents, specifically the Russians, attempted to interfere in American elections in 2016. The fact of Russian interference in the 2016 election was confirmed by eight credible national entities—the Central Intelligence Agency, the Office of the Director of National Intelligence, the Federal Bureau of Investigation, the National Security Agency, the Justice Department, the Department of Homeland Security and the House Intelligence Committee and Senate Intelligence Committee.

Not only was there consensus among American intelligence officials, even Democrats and Republicans both agreed that attempts were made by Russia to compromise the integrity of American elections. Only July 17, 2018, then House Speaker Paul Ryan said to reporters, "They did interfere in our elections—it's really clear," and Senate Majority Leader Mitch McConnell referred to "indisputable evidence" of Russia's attempts to influence the 2016 election.

Leader McConnell further stated, "We understand the Russian threat, and I think that is the widespread view here in the United States among Members of both parties."

More details of foreign interference in our election became known through the release of Special Counsel Robert Mueller's report, which detailed the following: "GRU officers [the main military foreign-intelligence service of Russia] also targeted individuals and entities involved in the administration of the elections. Victims included U.S. state and local entities, such as state boards of elections (SBOEs), Secretaries of State, and county governments, as well as individuals who worked for those entities. The GRU also targeted private technology firms responsible for

manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations."

In June 2017, then Democratic Leader Nancy Pelosi created the Congressional Task Force on Election Security in response to the then-Majority's inaction on the topic. Despite our clear responsibilities under House Rules, not a single hearing was held in this Committee on this topic last Congress. In February 2018, the Task Force released its report recommending reforms that could significantly advance election security. Among some of the proposed reforms are the replacement of paperless voting machines with paper ballot voting systems; risk-limiting audits; upgraded Information Technology infrastructure (including voter registration databases) with ongoing maintenance; requirements that election technology vendors secure their voting systems; Intelligence Community pre-election threat assessments and coordination with federal and state officials; and prioritized state-level cybersecurity trainings.

Congress has not done enough to tackle this problem. The risks posed by the vulnerabilities previously exploited still remain. Despite the overwhelming evidence showing these vulnerabilities the White House has failed to take these issues seriously and to direct resources towards securing election infrastructure. Last summer, in remarks to the National Association of Secretaries of State, former Homeland Security Secretary Kristjen Nielsen said that there were "no indications that Russia is targeting the 2018 U.S. midterms at a scale or scope to match their activities in 2016," but that she "consistently observed malicious cyber activity from various actors against U.S. election infrastructure.

She also said that "there is little doubt that adversaries and non-state actors continue to view elections as a target for cyber and influence operations." According to the New York Times, Nielsen "eventually gave up on her effort to organize a White House meeting of Cabinet Secretaries to coordinate a strategy to protect next year's elections. As a result, the issue did not gain the urgency or widespread attention that a President can command. And it meant that many Americans remain unaware of the latest versions of Russian interference." In spite of White House inaction, the Election Assistance Commission, in cooperation with the Department of Homeland Security, has been successful at building relationships with state officials and providing valuable resources as part of the "critical infrastructure" designation—but in the face of increasing threats, their efforts must expand.

However, such expansion is only possible if Congress increases their resources—today the EAC is operating with only half the budget and fewer than half the staff it had ten years ago, when threats were less grave. This already under-resourced agency is thus only further stymied by the White House's

strenuous efforts to avoid acknowledging our vulnerability, and the need to secure our elections from foreign threats—facts accepted as plan by both the legislative branch and national intelligence agencies. This is unacceptable, and several things must change. States need money to be able to replace their paperless voting machines and outdated IT infrastructure. States and localities also face the daunting task of training hundreds, if not thousands, of election officials, IT staff, and poll workers on cybersecurity and risk mitigation. Another significant vulnerability comes from election technology vendors. Many States purchase their voting systems from third-party vendors who have little financial incentive to prioritize election security and are not subject to regulations requiring them to use cybersecurity best practices.

Nor are they necessarily voluntarily adhering to these best practices: In July 2018, it was revealed that ES&S, one of the Nation's largest voting machine makers, had actually installed remote-access software on election management systems, although it had lied about this fact to the press. This fact was only uncovered through an inquiry by Senator Ron Wyden, who characterized this remote-access software installation "is the worst decision for security short of leaving ballot boxes on a Moscow street corner." In addition, election vendors are not currently required to inform any federal agency or state election official in the event of a cyberattack. Federal action is needed now to grasp the scope of the problem and to innovate concrete solutions that can be implemented before the next federal election cycle in 2020. That goal will be a primary focus of this Committee moving forward.

No matter your side of the aisle, the oath to upholding democracy as citizens and elected leaders in this Nation is fundamental. That is why I am glad to convene this hearing today, especially recognizing our new Ranking Member Rodney Davis' avowed commitment to advancing election security—so every voter can feel her vote is accurate, counted, and safe from the influence of those who wish to see our great democratic experience fail.

With that goal in mind, I welcome my fellow Members, all of you in the audience, and those who have come to share their expert testimony as witnesses. I look forward to hearing from you today.

Mr. DAVIS of Illinois. Thank you, Madam Chairperson, and thank you for your leadership of this Committee and your bipartisan leadership on this issue.

Election security is one of the most important issues that this Committee is tasked with and I take the responsibility of ensuring fair and secure elections extremely serious. I know that my colleagues on this Committee share—we share in this sentiment.

We know that at least 21 States were targeted by a foreign state actor prior to the 2016 U.S. election and we know that Russia undertook a misinformation campaign during the same election. I think I can safely say that everyone on this panel finds that troubling, but we must also factually say that no votes were changed in the 2016 election and that through the tremendous effort of local, State, and Federal officials, the 2018 midterm elections, with record midterm turnout, were secure—with record voter participation, once again. In fact, we saw the highest turnout in a midterm election in the last 50 years.

As we discuss election security today, it is important to note that many of the best practices used to protect our elections are noncontroversial. And I want to take a moment to clearly demonstrate what I am for. I am for an election system remaining—I am for election systems remaining as critical infrastructure. I am for helping our election technology vendors secure their voting systems. I am for ensuring our election officials, both at the State and Federal level receive security clearances in a timely manner. I am for empowering the Election Assistance Commission to lead our Federal support to State and local officials. I am for the Department of Homeland Security lending their expertise to State and local officials when appropriate.

We must also recognize that our States and the Federal Government have taken significant steps to carry out these practices and services. We can take a look at my home State of Illinois, which has invested in a new Cyber Navigator Program that helps counties detect and defend themselves against cybersecurity attacks. I believe we can cannot lose sight of what Chris Krebs, the Director of the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, said before the House Homeland Security Committee earlier this year. Director Krebs said, quote: "Local officials know their system and what they need to do to conduct a successful election, end quote, and State and local officials should remain in control of their elections."

As I have said many times, I believe that partisanship is the greatest threat to our elections. Election security cannot be a partisan exercise, but what we saw during the markup and passage of H.R. 1 was purely partisan. Too much is at stake to make this about party. If this hearing is an effort by my colleagues to take a bipartisan look at election security, I welcome it. We have important work to do here. However, I will not support any attempt today to waste an opportunity to work together and strengthen our election security for an attempt to make the nightly news with a partisan political agenda.

I look forward to learning from our witnesses today on best practices that States are implementing to combat foreign interference and secure our Nation's elections. I look forward to hearing more

about the tremendous effort of the Election Assistance Commission, the Department of Homeland Security, our two secretaries of state, representing the rest in the Nation, and most importantly, our local officials, where we see the safest, fairest, and the most secure elections being administered many, many times throughout the decade. I welcome all of the guests today and the witnesses. I look forward to hearing from you.

Madam Chairperson, I yield back.

[The statement of Mr. Davis of Illinois follows:]

Congress of the United States
House of Representatives
COMMITTEE ON HOUSE ADMINISTRATION
1309 Longworth House Office Building
Washington, D.C. 20515–6157
(202) 225–2061
https://cha.house.gov

Ranking Member Rodney Davis
Hearing on Election Security
May 8, 2019
Opening Statement

Thank you, Madam Chairperson. I'm thankful our Committee has decided to take up the important issue of election security.

I know I have little time, but I want to draw the Committee's attention to tools we should be looking at making more widely available in the election realm- such as WHOIS data (Who-is data) which has proven useful time and again at identifying the entities behind nefarious websites. Currently some domain name providers are restricting access to such data, and while our Federal agencies are working through diplomatic channels to reinstate access to WHOIS data, it is something we will want to watch closely to ensure we have the tools we need to secure our elections.

Securing our elections cannot be a partisan exercise. I have always been supportive of enhancing our election security, which is why I introduced an amendment during H.R. 1 discussions to replace Title III, the Majority's partisan attempt of election security, with the Senate's bipartisan bill, the Secure Elections Act.

Again, I think we can all agree on this panel that we have work to do when it comes to ensuring our elections are safe from interference, and I'm willing to work with my colleagues when they are ready to include us in discussion on future legislation. Thank you and I yield back.

The CHAIRPERSON. Thank you, Mr. Davis.

And other Members are welcome to submit their opening statements for the record.

I would now like to introduce our distinguished panel of witnesses.

Under the rules of this Committee, you have five minutes to present your oral testimony. However, your full written testimony will be made part of the record. There is a light system in the front. When you are down to one minute, it goes yellow from green. And when it is red, your time is up, and we would ask you to sum up. Let me introduce each witness, and then we will begin.

First, we have Lawrence Norden, who is the Deputy Director of the Brennan Center's Democracy Program. Mr. Norden has worked at the Brennan Center for some time, authoring several nationally recognized reports on election security. He served as chair of the Ohio Secretary of State's bipartisan election summit. He is the lead author of the book "Machinery of Democracy: Protecting Elections in the Electronic World." He has written extensively on the influence of money in New York State politics. He is a graduate of the University of Chicago and the NYU School of Law.

Next, we have Marian Schneider, who is the President of Verified Voting. She brings a strong grounding in the legal and constitutional elements governing voting rights in elections, as well as experience in election administration at the State level. She has served as a special advisor to Pennsylvania Governor Tom Wolf on election policy. Throughout her career, she has focused on the intersections of civil rights and election law. She received her Juris Doctor degree from George Washington University where she was a member of the Law Review and earned her Bachelor's of Arts degree cum laude from the University of Pennsylvania.

Next, we have Joseph Lorenzo Hall, the Chief Technologist and Director of the Internet Architecture Project at the Center for Democracy and Technology. His work has focused on the intersection of technology, law, and policy, working to ensure that technical considerations are appropriately embedded into legal and policy arguments. He also leads CDT's internet architecture project. Thank you very much for that. He has received numerous awards I cannot read them all, but prior to joining CDT in 2012, he was a post-doc research fellow at NYU, and he was at Princeton University, as well as the University of California, where he received his Ph.D. in information systems. His Ph.D. thesis used electronic voting as a critical case study in digital government transparency.

Next, we have Jocelyn Benson who is the Secretary of State of Michigan. We appreciate so much that you have made your way here. She was sworn in as Michigan's 43rd Secretary of State, January 21st, 2019, after being elected last November to a four-year term. Her focus for the department is customer service excellence. She is an expert on civil rights law, education law, and election law. She served as Dean of Wayne State University Law School in Detroit. When she was appointed dean at age 36, she became the youngest woman in U.S. history to lead a top-100 accredited law school. She continues to serve as Vice Chair of the advisory board for the Levin Center at Wayne Law which she founded with former Senator Carl Levin. Prior to her election, she served as CEO of the

Ross Initiative in Sports for Equality, otherwise known as RISE. She is the founder of the nonpartisan Michigan Center for Election Law. She earned a Bachelor of Arts from Wellesley College, a Master of Philosophy from Oxford University, and a law degree from Harvard Law School.

Finally, but certainly not least, we have John H. Merrill, the Secretary of State of Alabama. We are so grateful that you would make time to be here with us today. Secretary of State Merrill grew up in Heflin. He is an Eagle Scout. He was a graduate of the University of Alabama, where he served as president of the Student Government Association as an undergraduate. He was elected to represent the people of District 62 in the State House of Representatives with 87 percent of the vote, the highest percentage garnered by a candidate in any contested House race that year. He served as Secretary Treasurer of the House Republican caucus and was a member of the powerful Rules Committee, Economic Development and Tourism. He has been awarded the Silver Beaver by the Black Warrior Council of the Boy Scouts of America, as well as the Sunlight Foundations Award for the most effective Republican member of the Alabama House of Representatives. He was elected in November of 2014, as Alabama Secretary of State, with 65 percent of the vote, winning 53 of Alabama's 67 counties and was inaugurated Alabama's 53rd Secretary of State in 2015. He is active in his community, his church, and active also with the National Association of Secretaries of State, and we look forward to hearing from him and from all of you.

We will start first with you.

STATEMENTS OF LARRY NORDEN, DEPUTY DIRECTOR, BRENNAN CENTER'S DEMOCRACY PROGRAM; MARIAN SCHNEIDER, PRESIDENT, VERIFIED VOTING FOUNDATION; JOSEPH LORENZO HALL, CHIEF TECHNOLOGIST AND DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY; THE HONORABLE JOCELYN BENSON, SECRETARY OF STATE, STATE OF MICHIGAN; AND THE HONORABLE JOHN MERRILL, SECRETARY OF STATE, STATE OF ALABAMA

STATEMENT OF LARRY NORDEN

Mr. NORDEN. Thank you, Chairperson Lofgren, Ranking Member Davis, Members of the Committee for this opportunity to testify today. Chairperson Lofgren has recounted the scope of Russian attacks against our election infrastructure in 2016, but there are several reasons to believe we could face even more serious threats in 2020. We have seen the kind of damage a well-planned attack by Russian operatives can do against election infrastructure in Ukraine, Bulgaria, and elsewhere, where attackers have deleted critical election files, shut down websites, and even inserted a virus designed to declare the wrong result.

Worse, there are other nation-states we need to worry about. U.S. intelligence agencies have warned of potential attacks by China, North Korea, and Iran, and, indeed, the Chinese are alleged to have launched attacks against Indonesia and Australia just this year.

The good news is that we have made significant progress to secure our elections since 2016. Most importantly, policymakers and

election officials are acutely aware of the threats to our election infrastructure. There is better information sharing and resources sharing between Federal, State, and local agencies. In the last 2 years, more resources have been made available to secure our election infrastructure, not least of which was $380 million in HAVA grants that Congress provided in 2018. The vast majority of which has been allocated to critical security measures.

Despite this progress, there is far more to be done. First, we must replace aging and insecure voting machines. In a recent survey by the Brennan Center, local officials in 31 States told us that they must replace their equipment before the 2020 election, but two-thirds of those officials said that they did not have adequate funds to do so and this was after Congressional funds were appropriated. Too often these systems use outdated software that no longer receive security patches, and election officials are forced to turn to eBay for replacement parts because those parts are no longer manufactured. A particularly urgent security issue is phasing out paperless machines in the 11 States that still use them.

Second, we need implementation of robust post-election audits—a comparison of paper ballots to software totals that will provide a high level of confidence in the election outcome and that will correct a wrong voting outcome. Only 21 States currently have voter records for—paper records for every vote and conduct post-election audits, precertification, and only two conduct risk-limiting audits, which provide the high level of confidence that I mentioned.

The good news is that several States used the HAVA money that was appropriated to pilot risk-limiting audits in the last year, and several jurisdictions would like to do more of those this year. And we certainly should be doing everything we can in the coming months and years to ensure that these are conducted nationwide.

Third and finally, we must provide ongoing long-term support for maintaining and improving election cybersecurity. The Mueller report is a reminder that the election infrastructure we need to protect goes far beyond voting machines. The Brennan Center has long advocated that all States implement a process of continuous cybersecurity vulnerability assessments and mediation. While we estimate that the costs of these kinds of assessments should be no more than a few million dollars a year, obviously the cost of securing vulnerabilities that are identified by such assessments will cost more.

Local election offices are on the front lines in defending our election infrastructure against attacks, but often have the least amount of IT or cybersecurity support. Routine, ongoing funding of programs like the one Ranking Member Davis mentioned, the Illinois Cyber Navigator Program, which directs personnel and resources to local offices, would help close that security gap.

It is cliché to say that this is a race without a finish line. Funding election security should be a shared responsibility among local, State, and the Federal level, but only Congress has the power to ensure that responsibility is shared by providing matching grants for State and local governments. I am hopeful to see a continued commitment from Congress to partner in this effort. Thank you.

[The statement of Mr. Norden follows:]

BRENNAN
CENTER
FOR JUSTICE

Committee on House Administration
United States House of Representatives

Statement of Lawrence D. Norden
Deputy Director, Democracy
Program,
Brennan Center for Justice at NYU School of Law

May 8, 2019

"Election Security"

Chairperson Lofgren, Ranking Member Davis, and members of the Committee, thank you for the opportunity to speak about the critical issue of election security. The Brennan Center for Justice—a nonpartisan law and policy institute that focuses on democracy and justice—appreciates the opportunity to share with you the results of our extensive studies and efforts to ensure our nation's election systems are more secure and reliable. We are deeply involved in the effort to ensure accurate and fair voting for all Americans.

For more than a decade, I have led the Brennan Center's extensive work on voting technology and security. In 2005, in response to growing public concern over the security of new electronic voting systems, I chaired a task force (the "Security Task Force") of the nation's leading technologists, election experts, and security professionals assembled by the Brennan Center to analyze the security and reliability of the nation's electronic voting machines.[1] In the decade and a half since, I have authored or co-authored numerous studies on election system security and technology, including the results of a semi-regular Brennan Center survey of the nation's roughly 8,000 local election officials.[2]

Our most recent survey (published in March) showed that while officials have made great progress

---

[1] "About the Task Force on Voting System Security," Brennan Center for Justice, January 1, 2005, https://www.brennancenter.org/analysis/about-task-force-voting-system-security.

[2] *See e.g.* Lawrence Norden, *Post-Election Audits: Restoring Trust in Elections,* Brennan Center for Justice, 2007, https://www.brennancenter.org/sites/default/files/legacy/d/download_file_50228.pdf; Lawrence Norden, *Voting System Failures: A Database Solution*, Brennan Center for Justice, 2010, https://www.brennancenter.org/sites/default/files/legacy/Democracy/Voting_Machine_Failures_Online.pdf; Lawrence Norden and Christopher Famighetti, *America's Voting Machines at Risk*, Brennan Center for Justice, 2015, https://www.brennancenter.org/publication/americas-voting-machines-risk; Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, https://www.brennancenter.org/publication/securing-elections-foreign-interference; Lawrence Norden and Wilfred U. Codrington III, "America's Voting Machines at Risk – An Update," *Brennan Center for Justice*, March 8, 2018, https://www.brennancenter.org/analysis/americas-voting-machines-risk-an-update; Lawrence Norden and Andrea Córdova, "Voting Machines at Risk: Where We Stand Today," *Brennan Center for Justice*, March 5, 2019, https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.

in the last two years toward improving election security, much work remains to be done.[3] In particular, local election officials around the country, underfunded and often without any local IT support, are on the front lines in the effort to protect our democracy against hostile actors, including foreign powers. They deserve leadership and resources from all levels of government.

I hope to convey three points in my testimony today:

(1) The United States has made important progress since 2016 in protecting its election infrastructure;
(2) While Special Counsel Robert Mueller's report confirmed a "sweeping and systemic" attack on American elections in 2016, there are several reasons to believe the threat against our election infrastructure will be even greater in 2020; and
(3) There is more to do to protect our elections in 2020 and beyond, and Congress has a critical leadership and partnership role to play.

A. The Attack Against America's Election Infrastructure in 2016 and the Progress We Have Made Since

The redacted Report on the Investigation into Russian Interference in the 2016 Presidential Election by Special Counsel Robert S. Mueller III (the Special Counsel's Report) is a powerful reminder and warning, just 18 months before our next presidential election, that a foreign power engaged in a major effort to interfere in our elections. The Special Counsel's Report confirms the reports of our intelligence agencies, as well as the results of Congressional investigations, which have shown that in addition to a massive effort on social media, the Russians targeted state and local election boards, breached and extracted data from a state registration database, and used spear phishing attacks to gain access to and infect computers of a voting technology company and at least one Florida county.[4]

Yet there is good reason to believe we face even more serious threats in 2020 and beyond. In contrast to other Russian efforts during the 2016 election cycle, the attacks against our election infrastructure appear to have begun relatively late compared to other aspects of their campaign, with the first documented intrusions noted in June of 2016. By 2020, the Russians will have had four years to leverage knowledge gained in 2016 to do more harm. Chris Krebs, head of the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security, has warned that the 2020 election is "the big game" for adversaries looking to attack American democracy.[5]

We have seen the kind of damage Russian operatives can do with well-planned attacks against election infrastructure, such as the alleged attacks against Ukraine's elections in 2014, which deleted enough files to make the country's voting system inoperable days before the election,

---

[3] Lawrence Norden and Andrea Córdova, "Voting Machines at Risk: Where We Stand Today," *Brennan Center for Justice*, March 5, 2019, https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.
[4] Robert S. Mueller III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, U.S. Department of Justice, 2019, 51, https://www.justice.gov/storage/report.pdf.
[5] Colleen Long and Michael Balsamo, "Cybersecurity officials start focusing on the 2020 elections," *Associated Press*, November 8, 2018, https://www.apnews.com/cfaa16f6a86349bebc16e0633d6214dd.

and which inserted a virus into the country's election night reporting designed to falsely declare an ultra-nationalist party as the victor.[6] We have seen similar attacks by alleged Russian operatives against Bulgaria's Central Election Commission during a referendum and local elections in 2015, as well as against Ukraine's election commission in 2019.[7]

Just as importantly, there are other nation-states that could attack our election infrastructure in 2020. U.S. national security agencies have warned of the potential for attacks against our elections from China, North Korea, and Iran, as well as non-state actors.[8] Since 2016, there have been reports of alleged Chinese election-related attacks against Indonesia's voter database[9] as well as against Australia's major political parties.[10]

There was a time when many assumed no nation-state would dare attack America's election infrastructure for fear of the consequences. We can no longer live under this illusion.

The good news is we have made significant progress since 2016 to secure our elections. Most importantly, policymakers and election officials around the country are acutely aware of the threat that hostile actors pose to the integrity of our elections. As a result, election officials and their employees have voluntarily participated in thousands of hours of cybersecurity trainings and table-top exercises to prevent, detect, and recover from intrusions into critical election infrastructure.[11]

The designation by the Department of Homeland Security ("DHS") of election infrastructure as critical infrastructure has meant that state and local election offices have had access to needed resources, including cybersecurity advisors and risk assessments. Meanwhile, DHS and the Election Assistance Commission ("EAC") have facilitated much better information sharing between election system vendors, the states, and the federal government.

Finally, in 2018 Congress provided $380 million in Help America Vote Act (HAVA) funds to help states bolster their election security. Based on information provided by the EAC, we know

---

[6] Andy Greenberg, "How an entire nation became Russia's test lab for cyberwar," *Wired*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

[7] Gordon Corera, "Bulgaria warns of Russian attempts to divide Europe," *BBC News*, November 4, 2016, https://www.bbc.com/news/world-europe-37867591; Pavel Polityuk, "Exclusive: Ukraine says it sees surge in cyber attacks targeting election," *Reuters*, January 25, 2019, https://www.reuters.com/article/us-ukraine-cyber-exclusive/exclusive-ukraine-says-it-sees-surge-in-cyber-attacks-targeting-election-idUSKCN1PJ1KX.

[8] *See, e.g.*, Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, Office of the Director of National Intelligence U.S.A, 2019, 6-7, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf; Jordan Fabian, "US warns of 'ongoing' election interference by Russia, China, Iran," *The Hill*, October 19, 2018, https://thehill.com/policy/national-security/412292-us-warns-of-ongoing-election-interference-by-russia-china-iran.

[9] Viriya Singgih, Arys Aditya, and Karlis Salna, "Indonesia Says Election Under Attack From Chinese, Russian Hackers," *Bloomberg*, March 13, 2019, https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers.

[10] Dean Pennington, "Australia's major parties targeted in 'sophisticated' cyber attack ahead of election," *TechSpot*, February 18, 2019, https://www.techspot.com/news/78802-australia-major-parties-targeted-ophisticated-cyber-attack-ahead.html.

[11] John V. Kelly, *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure*, Office of Inspector General, Department of Homeland Security, February 18, 2019, https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf.

that the vast majority of this money is being used to strengthen election cybersecurity, purchase new voting equipment, and improve post-election audits, all essential steps that experts have agreed need immediate action.[12]

B. There is Critical Work to be Done Ahead of the 2020 Election and Beyond

Despite this progress, there is far more work that needs to be done to improve the security of our elections in 2020 and beyond. I submit there are four main areas that deserve special attention, which I will discuss in detail below: (1) replacement of aging and insecure voting machines, particularly paperless systems, which experts agree should be removed from service as soon as possible; (2) widespread implementation of post-election audits that will provide a high level of confidence in the accuracy of the final vote tally; (3) upgrading or replacing election-related computer systems to address cyber vulnerabilities identified by DHS or similar scans or assessments of existing election systems; and (4) increased training and IT resources for state and local election officials. Many of these items are addressed in provisions of H.R. 1, Titles I and III, as well as other bills introduced in the last year by Republicans and Democrats.[13] Passage of these provisions would be a tremendous step forward towards securing our elections.

1. Many Localities Need to Replace Their Voting Machines Before 2020, and This is Particularly Urgent in States That Still Use Paperless Systems

In late 2015, the Brennan Center published *America's Voting Machines at Risk*, a comprehensive look at the voting systems used in the United States.[14] In that report, we warned of the impending crisis as voting machines around the country aged, presenting serious security and reliability challenges.

Our concern about the continued use of these systems was and is threefold. First, older systems are more likely to fail and are increasingly difficult to maintain. This was borne out in the 2018 midterm election, when old and malfunctioning voting machines across the country created long lines at the polls, leaving voters frustrated – and, in some cases, causing them to leave before casting a ballot.[15]

---

[12] *Grant Expenditure Report, Fiscal Year 2018*, The U.S. Election Assistance Commission, April 4, 2019, https://www.eac.gov/assets/1/6/FY2018HAVAGrantsExpenditureReport.pdf.

[13] See, e.g., For the People Act of 2019, H.R.1, 116th Cong. (2019); Election Security Act, H.R.5011, 115th Cong. (2018); Protecting the American Process for Election Results (PAPER) Act, H.R.3751, 115th Cong. (2017); Secure Elections Act, S.2261, 115th Cong. (2017).

[14] Lawrence Norden and Christopher Famighetti, *America's Voting Machines at Risk*, Brennan Center for Justice, 2015, https://www.brennancenter.org/publication/americas-voting-machines-risk.

[15] Erik Ortiz, Shamar Walters, Emily Siegel, Jareen Imam, Sarah Fitzpatrick, and Alex Johnson, "Midterms 2018: Voters face malfunctioning machines and long lines at polls across country on Election Day," *NBC News*, November 6, 2018, https://www.nbcnews.com/politics/elections/midterms-2018-voters-face-malfunctioning-machines-long-lines-polls-across-n932156; Ashley Lopez, "Old Voting Machines Confuse Some Texans During Midterm Election," *NPR*, October 30, 2018, https://www.npr.org/2018/10/30/662095109/old-voting-machines-confuse-some-texans-during-midterm-election; Christina A. Cassidy, Colleen Long, and Michael Balsamo, "Machine breakdowns, long lines mar vote on Election Day," *Associated Press*, November 6, 2018, https://www.apnews.com/6fb6de6fdb034b889d301efd12602e21; P.R. Lockhart, "Voting hours in parts of Georgia extended after technical errors create long lines," *Vox*, November 6, 2018, https://www.vox.com/policy-and-politics/2018/11/6/18068492/georgia-voting-gwinnett-fulton-county-machine-problems-midterm-election-extension.

Second, aging voting systems also use outdated hardware and software and many of them are no longer manufactured. This can make finding replacement parts difficult, if not impossible. In several cases, officials have had to turn to eBay to find critical components like dot-matrix printer ribbons, decades old memory storage devices and analog modems.[16] Aging systems also frequently rely on unsupported software, like Windows XP and 2000, which may not receive regular security patches and are thus more vulnerable to the latest methods of cyberattack.[17]

Third, older systems are less likely to have the kind of security features we expect of voting machines today. While nearly all of today's new voting machines go through a federal certification and testing program, many jurisdictions using older equipment purchased their voting machines before this process was in place. Older machines can have serious security flaws, including hacking vulnerabilities, which would be unacceptable by today's standards.

Most notably, older systems disproportionately do not employ voter-marked paper ballots that can be used to detect and recover from attacks on voting machine software. The National Academy of Sciences, Engineering, and Medicine is just one of the latest authorities to examine such systems and conclude that they should be "removed from service as soon as possible" to ensure the security and integrity of American elections.[18] They have been joined in this conclusion by the U.S. Senate Select Committee on Intelligence, as well as security experts around the country, all of whom have argued that continued use of these systems presents an unnecessary security risk.[19]

Since our 2015 report, several states have made significant progress in replacing antiquated equipment. In particular, Colorado, Michigan, Ohio and Rhode Island are among the states that have replaced all or a significant portion of their aging voting equipment. Perhaps most importantly, Virginia, Arkansas, and Delaware have completely replaced their paperless voting machines with systems that use voter-marked paper ballots, and other states, including Georgia,

---

[16] Mark Earley (Voting Systems Manager, Leon County, Florida) interview by Brennan Center, January 26, 2015; Paul Ziriax (Secretary, Oklahoma Board of Elections) and Pam Slater (Assistant Secretary, Oklahoma Board of Elections), interview by Brennan Center March 16, 2015; Kristin Mavromatis (Public Information Manager, Mecklenburg County, North Carolina) interview by Brennan Center, April 9, 2015. *See* Lawrence Norden and Christopher Famighetti, *America's Voting Machines at Risk*, Brennan Center for Justice, 2015, 14 , https://www.brennancenter.org/publication/americas-voting-machines-risk.

[17] For instance, Microsoft stopped supporting Windows XP in 2014, with the exception of a "highly unusual patch" that it issued in 2017 to prevent the spread of WannaCry malware. *See* Tom Warren, "Microsoft releases new Windows XP security patches, warns of state-sponsored cyberattacks," *The Verge*, June 13, 2017, https://www.theverge.com/2017/6/13/15790030/microsoft-windows-xp-vista-security-updates-june-2017.

[18] *Securing the Vote: Protecting American Democracy,* The National Academies of Sciences, Engineering, and Medicine, 2018, 5, https://www.nap.edu/read/25120/chapter/1.

[19] *Securing the Vote: Protecting American Democracy,* The National Academies of Sciences, Engineering, and Medicine, 2018, https://www.nap.edu/read/25120/chapter/1; *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*, U.S. Senate Select Committee on Intelligence, May 8, 2018, https://www.intelligence.senate.gov/publications/russia-inquiry; Danielle Root, Liz Kennedy, Michael Sozan, and Jerry Parshall, *Election Security in All 50 States: Defending America's Elections*, Center for American Progress, February 12, 2018, https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/; "Study and Recommendations," The Blue Ribbon Commission on Pennsylvania's Election Security, 2019, 21, https://www.cyber.pitt.edu/sites/default/files/FINAL%20FULL%20PittCyber_PAs_Election_Security_Report.pdf.

Louisiana, New Jersey, South Carolina, and Pennsylvania, have taken important steps to replace this equipment.[20]

This winter, the Brennan Center surveyed election officials around the country on their need to replace their voting machines. Local officials in 31 states told us that they must replace their equipment before the 2020 election, but two-thirds of these officials said that they do not have the adequate funds to do so, even after the distribution of additional HAVA funds from Congress.[21] Meanwhile, officials in 40 states told us they are using at least some voting machines that are more than a decade old this year, perilously close to the end of the lifespan for many of these systems.[22] And officials in 45 states currently use at least some systems that are no longer manufactured, with many reporting that they have difficulty finding replacements when parts fail.[23] There should be little doubt that most of these machines will need to be replaced in the

---

[20] The Verifier — Polling Place Equipment — November 2018," Verified Voting, accessed February 22, 2019, https://www.verifiedvoting.org/verifier/; Delaware will start rolling out machines with paper backups on May 14 of this year. *See* Amy Cherry, "Delawareans to get 1st look at new voting machines in upcoming school board elections," *WDEL*, May 6, 2019, https://www.wdel.com/news/video-delawareans-to-get-st-look-at-new-voting-machines/article_7d625346-6ddd-11e9-a2c7-4f6dfafa74af.html; Kim Wade, "Georgia Sec. of State seeks to replace criticized voting machines," *WSAV*, January 24, 2019, https://www.wsav.com/news/local-news/georgia-sec-of-state-seeks-to-replace-criticized-voting-machines/1722859964; Mark Niesse, "Voters Confront Georgia Lawmakers Over New Touchscreen Election System," *WSB Radio*, February 19, 2019, https://www.wsbradio.com/news/state--regional-govt--politics/voters-contront-georgia-lawmakers-over-new-touchscreen-election-system/Jj26WLlCuMXKuzL6nZo9oI/; Melinda Deslatte, "Kyle Ardoin wins election for Louisiana secretary of state," *Associated Press*, December 8, 2018, https://www.apnews.com/782bb812689045328f876dd300f08840; Meghan Grant, "Some NJ voters will cast their next ballot on new, more secure voting machines," *North Jersey Record*, March 11, 2019, https://www.northjersey.com/story/news/new-jersey/2019/03/11/new-nj-voting-machine-pilots-being-rolled-out-across-state/1266947002/; Bristow Marchant, "SC takes first step toward switching to paper ballots in 2020," *The State*, January 15, 2019, https://www.thestate.com/news/politics-government/article224557350.html; Marc Levy, "Pennsylvania must replace voting machines, lawmakers told," *AP News*, February 20, 2019, https://www.apnews.com/15e507d74d0e439faf775cc45bb0aa7d.

[21] In our survey, election officials in 31 states (Arizona, Arkansas, California, Colorado, Delaware, Florida, Georgia, Illinois, Iowa, Kansas, Maine, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Nebraska, New Hampshire, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, West Virginia, Wisconsin, and Wyoming) told us they needed to replace their voting machines by 2020. *See* Lawrence Norden and Andrea Córdova, "Voting Machines at Risk: Where We Stand Today," *Brennan Center for Justice*, March 5, 2019, https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.

[22] In our survey, jurisdictions from 40 states (Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming) told us that their voting machines were at least a decade old. *See* Lawrence Norden and Andrea Córdova, "Voting Machines at Risk: Where We Stand Today," *Brennan Center for Justice*, March 5, 2019, https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.

[23] The Brennan Center confirmed with three major vendors (ES&S, Dominion, and Hart InterCivic) that the following models are no longer manufactured: iVotronic, M100, M650, AutoMark (ES&S); AccuVote OS, AccuVote OSX, AccuVote TS, AccuVote TSX, AVC Edge, AVC Advantage, Optech IIIP-Eagle and Optech Insight (Dominion); eScan, eSlate and Judge's Booth Controller (Hart Intercivic). Danaher's Shouptronic 1242, used mainly in Delaware, is also no longer manufactured. We used this information to confirm that seven states (Delaware, Georgia, Hawaii, Louisiana, North Dakota, Oklahoma, and South Carolina) are using exclusively discontinued voting machines, 38 states (Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Florida, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Massachusetts, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New York, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming) use

coming years.

Nearly 100 percent of election officials who hoped to replace their machines before 2020 stated that they intend to replace their systems with machines that produced a voter-verifiable paper record that could be used to detect and recover from an attack on voting system software. And yet, while several states have passed laws or taken steps to replace paperless voting machines before 2020, most have not yet secured sufficient funds for local election officials to do so. Today, 11 states still use paperless electronic machines as the primary polling place equipment in at least some counties and towns (Georgia, Indiana, Kansas, Kentucky, Louisiana, Mississippi, New Jersey, Pennsylvania, South Carolina, Tennessee and Texas). Three (Georgia, Louisiana, and South Carolina) continue to use such systems statewide.[24]

The Brennan Center has estimated it would cost more than $300 million to replace all remaining paperless voting machines in the United States and more than $700 million to replace voting machines that are currently over a decade old.[25]

2. More States Should Conduct Robust Post-Election Audits

As the Brennan Center noted in its 2006 report *The Machinery of Democracy*, moving to paper-based systems without using the paper to check the accuracy of electronic totals may be of "limited security value."[26] Paper records will not prevent programming errors, software bugs, or the insertion of corrupt software into voting systems. Voter-marked paper ballots will only have real security value if they are used to check and confirm electronic tallies.[27]

Since the issuance of that report, we have made tremendous strides in developing post-election audits that can efficiently allow us to detect and recover from a software hack or bug that could alter an election outcome. In particular, post-election risk-limiting audits (RLAs) require hand

---

discontinued voting machines in one or more jurisdictions, and five states (Maine, Maryland, Michigan, Nevada, New Mexico) and the District of Columbia use machines that are all currently manufactured. See Kathy Rogers, (Senior Vice President of Government Relations, ES&S), Conversation with Edgardo Cortez, February 13, 2019; Kay Stimson (Vice President, Government Affairs, Dominion), Email message to Edgardo Cortez, Feb 27, 2019; Sam Derheimer (Director of Government Affairs, Hart InterCivic), Email message to Edgardo Cortez, Feb 14, 2019; "Danaher Shouptronic 1242," Verified Voting, accessed February 25, 2019, https://www.verifiedvoting.org/resources/voting-equipment/danaher/shouptronic/; "The Verifier — Polling Place Equipment — November 2018," Verified Voting, accessed February 25, 2019, https://www.verifiedvoting.org/verifier/.

[24] "The Verifier — Polling Place Equipment — November 2018," Verified Voting, accessed May 6, 2019, https://www.verifiedvoting.org/verifier/.

[25] "Estimate for the Cost of Replacing Paperless, Computerized Voting Machines," Brennan Center for Justice, 2018, https://www.brennancenter.org/sites/default/files/analysis/New_Machines_Cost_Across_Paperless_Jurisdictions%20%282%29.pdf; Relying on Verified Voting data from November 2018, we estimated that 90,140 precincts are using voting machines that are at least 10 years old. We multiplied this number of precincts by $8,000, our estimate for per-precinct machine replacement cost, to arrive to our $700 million estimate.

[26] Lawrence Norden, *The Machinery of Democracy: Protecting Elections In An Electronic World*, Brennan Center for Justice, 2006, https://www.brennancenter.org/sites/default/files/publications/Machinery%20of%20Democracy.pdf.

[27] Ibid.

counts of statistical samples of voter verifiable paper ballots. In the words of the EAC, such audits provide "strong statistical evidence that the election outcome is right and has a high probability of correcting a wrong outcome,"[28] and are thus a critical measure for increasing the public confidence in and integrity of our elections.

Unfortunately, only 22 states that have paper records of every vote require post-election audits of those votes before certifying their elections.[29] This is only two more than did so in 2016.[30] Even in states where post-election audits are required, in most cases they could be far more robust; only two, Colorado and Rhode Island, will require RLAs in 2020.

Still, it is clear that more jurisdictions are hoping to expand the use of RLAs. Three additional states—California, Ohio, and Washington—allow election officials to select them from a list of audit types.[31] Georgia recently passed a law that would require RLAs beginning in 2021.[32] Bills to require RLAs or authorize RLA pilots are also pending in New York, Indiana, South Carolina, and New Jersey.[33] Several more jurisdictions have recently piloted these post-election audits, and even more intend do so in 2019. This includes election jurisdictions in Michigan, New Jersey, Rhode Island, Virginia, Indiana and California.[34] A number of these jurisdictions used the 2018 Congressional HAVA grants to conduct the pilots.[35]

---

[28] Jerome Lovato, "Defining and Piloting Risk-Limiting Audits," *U.S. Election Assistance Commission*, accessed May 6, 2019, https://www.eac.gov/defining-and-piloting-risk-limiting-audits-/.

[29] These twenty-two states are Alaska, Arizona, California, Colorado, Connecticut, Hawaii, Illinois, Iowa, Massachusetts, Minnesota, Missouri, Montana, Nevada, New Mexico, New York, North Carolina, Ohio, Oregon, Rhode Island, Utah, Washington, and West Virginia. Although Ohio conducts post-election audits after certification, the Election Board must amend its certification if the audit results in a change of the vote totals reported in the official canvass; *See* "POST-ELECTION AUDITS," National Conference of State Legislatures, last modified February, 1, 2019, accessed May 6, 2019, http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx ; Danielle Root, Liz Kennedy, Michael Sozan, and Jerry Parshall, *Election Security in All 50 States: Defending America's Elections*, Center for American Progress, February 12, 2018, https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/.

[30] 17 R.I. Gen Laws §17-19-37.4 (2017); 2017 Iowa Acts 256.

[31] *CAL. ELEC CODE* §15365-15367; *Ohio Election Official Manual*, Ohio Secretary of State, August 1, 2018, https://www.sos.state.oh.us/globalassets/elections/directives/2017/dir2017-10_eom.pdf/; WASH. REV. CODE ANN. §29A.60.185.

[32] H.B 316, 2019 Gen. Assemb., Reg. Sess. (Ga. 2019).

[33] S.B. 2329, 2019 Leg., Reg. Sess. (Ny. 2019); S.B. 405, 121st Gen. Assemb., Reg. Sess. (In. 2019); H.B 3304, 2019 Gen. Assemb. 123rd Sess. (Sc. 2019); A.B. 3991, 218th Leg., (Nj. 2018).

[34] Kellie Ottoboni, "Piloting Risk-Limiting Audits in Michigan," *Berkeley Institute for Data Science*, December 20, 2018, https://bids.berkeley.edu/news/piloting-risk-limiting-audits-michigan; Abigail Abrams, "Russia Wants to Undermine Trust in Elections. Here's How Rhode Island Is Fighting Back," *Time Magazine*, January 26, 2019, http://time.com/5510100/risk-limiting-audit-election-security/; *Risk-Limiting Audits,* Department of Elections, Virginia, September 20, 2018, https://www.elections.virginia.gov/media/Media/Agendas/2018/20180920-RLA_Report.pdf; Stephanie Singer and Neal McBurnett, *Orange County, CA Pilot Risk-Limiting Audit*, Verified Voting, December 7, 2018, https://www.verifiedvoting.org/wp-content/uploads/2018/12/2018-RLA-Report-Orange-County-CA.pdf.

[35] Abigail Abrams, "Russia Wants to Undermine Trust in Elections. Here's How Rhode Island Is Fighting Back," *Time Magazine*, January 26, 2019, http://time.com/5510100/risk-limiting-audit-election-security/ Colleen O'Dea, "Progress seen in test of paper-trail voting machines that allow audit of results," *NJ Spotlight*, January 4, 2019, https://www.njspotlight.com/stories/19/01/03/progress-seen-in-test-of-paper-trail-voting-machines-that-allow-audit-of-results/.

The Brennan Center has strongly encouraged all states to adopt robust post-election audits. More pilots of RLAs, in particular, will help to get us to a point where we can conduct these nationwide and have a high level of confidence that a software bug, error, or hack did not change the outcomes of federal contests. We believe Congress should take steps to encourage states and localities to adopt this critical security measure.

3. States and Counties Must Upgrade or Replace Election-Related Computer Systems and Websites Where Vulnerabilities are Discovered

The Special Counsel's Report makes clear that there is a much larger infrastructure than just voting machines that we need to protect from cyberattack. Indeed, if we look at incursions into election systems in the United States and abroad over the last few years, including since 2016, we see some of the most common targets are election officials' e-mail, state and locality voter registration databases, election night reporting, and other election websites.[36]

At least 21 states have requested Risk and Vulnerability Assessments of their election-related networks and computer systems from DHS, and several additional states have contracts with private vendors to conduct assessments of the entirety of their election-related computer systems.[37] The Brennan Center has advocated that all states implement a process of continuous cybersecurity vulnerability assessments. While we estimate the cost of such assessments will be no more than a few million dollars annually, the cost of securing vulnerabilities identified by such assessments is likely to cost many millions more.[38]

Without question, one of the most important and costly sets of systems to secure – through upgrades or replacements – will be state and local voter registration databases. Indeed, many registration systems in the United States are as old as or older than voting systems in use today. If anything, the use of outdated databases and operating systems presents even more challenges than those associated with using old voting machines. As Marc Burris, Chief Information Officer of the North Carolina State Board of Elections put it, at least the oldest voting machines in the

---

[36] Pavel Polityuk, "Exclusive: Ukraine says it sees surge in cyber-attacks targeting election," *Reuters*, January 25, 2019, https://www.reuters.com/article/us-ukraine-cyber-exclusive/exclusive-ukraine-says-it-sees-surge-in-cyber-attacks-targeting-election-idUSKCN1PJ1KX; Viriya Singgih, Arys Aditya, and Karlis Salna, "Indonesia Says Election Under Attack From Chinese, Russian Hackers," *Bloomberg*, March 13, 2019, https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers; Benjamin Wofford, "The hacking threat to the midterms is huge. And technology won't protect us," *Vox*, October 25, 2018, https://www.vox.com/2018/10/25/18001684/2018-midterms-hacked-russia-election-security-voting; Lynn Sweet, "Mueller report confirms Russians 'compromised' Illinois State Board of Elections," *Vox*, April 18, 2019, https://chicago.suntimes.com/news/mueller-report-special-counsel-russia-hacking-illinois-state-board-elections/.

[37] Chris Good, "Fewer than half of US states have undergone federal election security reviews ahead of midterms," *ABC News*, October 30, 2018, https://abcnews.go.com/Politics/fewer-half-us-states-undergone-federal-election-security/story?id=58858453.

[38] Matt Damschroder, (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden; Edgardo Cortes (Commissioner, Department of Elections, Virginia), email message to Lawrence Norden, June 20, 2017, *See* Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, 19, https://www.brennancenter.org/publication/securing-elections-foreign-interference; Robert A. Brehm (Co-Executive Director, New York State Board of Elections), interview by Brennan Center for Justice, May 6, 2019; Mandy Vigil (Acting Elections Director, New Mexico Secretary of State), interview by Brennan Center for Justice, May 6, 2019.

United States were actually "designed for a longer shelf life. That's not true of many of the database systems we are using today."[39]

In September 2015, the Brennan Center estimated that 41 states were using voter registration databases that were initially created at least a decade ago. While some states have since replaced or substantially upgraded their systems, most have not.[40] In the past decade, of course, cyber threats have advanced enormously. As Edgardo Cortés, former Commissioner for the Virginia Department of Elections and Brennan Center Election Security Advisor, has noted, "These systems weren't designed with [current cyber threats] in mind." Officials from a number of states, including Arizona, Minnesota, New Jersey, and Pennsylvania, have stated that they hope to invest in improving or replacing their voter registration systems in the very near future.

The need for updates or replacement of IT infrastructure and software may be even greater at the local level, where systems often run on discontinued software like Windows XP or Windows 2000 that is more vulnerable to cyberattack because it is no longer vendor supported. This is particularly troubling because smaller jurisdictions frequently have little or no IT support of their own. As Matt Damschroder (former Assistant Secretary of State in Ohio) has noted, "at the state level, you are generally going to have more resources and higher levels of sophistication."[41] Local election officials are likely to have "far fewer resources" to protect against attacks.

4. Local Election Jurisdictions Need More Cybersecurity Resources

The vast and decentralized election system in the United States means our elections are largely run at the local level. While there are certainly security benefits associated with this decentralization,[42] there are also obvious risks. Foremost among these is the fact that with over 8,000 separate election offices, there are many potential targets. As Bob Brehm, Co-Executive Director of the New York State Board of Elections, recently put it in an interview with the Brennan Center, "it is not reasonable" to expect each of these state and local election offices to independently "defend against hostile nation-state actors."[43] This is particularly true in the case of local election offices that frequently have little or no in-house IT or cybersecurity resources.

---

[39] Marc Burris (IT Director and CIO, State Board of Elections, North Carolina), in phone discussion with Lawrence Norden, May 22, 2017, *See* Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, 19, https://www.brennancenter.org/publication/securing-elections-foreign-interference.

[40] "California Secretary of State Certifies Centralized Statewide Voter Registration System," *Government Technology*, September 28, 2016, https://www.govtech.com/computing/California-Secretary-of-State-Certifies-Centralized-Statewide-Voter-Registration-System.html; "In November of 2017, a contract was issued to Sutherland Government Solutions, Inc. for the acquisition of a new statewide voter registration database ("AVID") that will replace our currently aging system ("VRAZII") on or before June 30, 2019," *See Arizona: 2018 HAVA Election Security Funds*, Arizona Secretary of State, 2018, 2, https://www.eac.gov/havadocuments/AZ_Narrative_Budget.pdf.

[41] Matt Damschroder, (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden, *See* Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, 20, https://www.brennancenter.org/publication/securing-elections-foreign-interference.

[42] *See* Dr. Dan S. Wallach, Testimony Before the House Committee on Space, Science & Technology Hearing 4, September, 13, 2016, https://www.cs.rice.edu/~dwallach/pub/us-house-sst-voting-13sept2016.pdf.

[43] Robert A. Brehm (Co-Executive Director, New York State Board of Elections), interview by Brennan Center for Justice, May 6, 2019.

I want to highlight two steps that states have already taken which, if adopted nationally, could bring greater cybersecurity protection to our local election offices. The first is the creation of statewide "cyber navigator" or cyber liaison programs for local election offices. As DHS has noted, "the purpose of these navigators is to provide practical cybersecurity knowledge, support and services to local election officials who otherwise would not have them."[44]

The state of Illinois recently allocated at least $7 million to create a cyber navigator program for its local election offices. Among other things, this money will be used to support 9 cyber navigators, assigned to geographic zones, who go into county clerks' offices to conduct trainings, risk assessments and evaluations to determine what type of equipment and software upgrades will be necessary, as well as to serve as a resource for county election offices going forward.

Illinois was able to use much of the HAVA funding it received in 2018 to launch its cyber navigator program. Other states like Alaska, Arkansas, Delaware, Louisiana, and Pennsylvania, which had to use their funds toward replacement of their paperless voting machines, will not have the luxury of using those funds for these purposes.

New York has chosen to use their HAVA funds to purchase intrusion detection services for all county election offices. New York State is spending $5 million to provide these services to all counties that were not provided with them for free under a program offered by the Elections Infrastructure Sharing Analysis Center (EI-ISAC) run by Center for Internet Security with support from DHS.[45] In interviews by the Brennan Center with local election officials, the desire for these kind of detection services has come up repeatedly.[46]

C. Congress Has a Critical Role to Play as Partner and Leader

Congress has a critical role to play, both in partnering with states and local governments by funding needed security steps, and providing direction about how that federal money should be used. As Michael Chertoff and Grover Norquist have put it, "Congress should recognize that election cybersecurity reforms are in their own personal interest – and in the interest of the United States national security."[47]

---

[44] *DHS Election Infrastructure Security Funding Consideration*, National Protection and Programs Directorate Department of Homeland Security, June 13, 2018, 2, https://www.dhs.gov/sites/default/files/publications/Election%20Infrastructure%20Security%20Funding%20Considerations%20Final.pdf.

[45] Robert A. Brehm (Co-Executive Director, New York State Board of Elections), interview by Brennan Center for Justice, May 6, 2019.

[46] Dana Debeauvoir (County Clerk, Travis County, Texas), interview by Brennan Center for Justice, February 14, 2019. *See* Lawrence Norden and Andrea Córdova, "Voting Machines at Risk: Where We Stand Today," *Brennan Center for Justice*, March 5, 2019, https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.

[47] Michael Chertoff and Grover Norquist, "We need to hack-proof our elections. An old technology can help," *The Washington Post*, February 14, 2018, https://www.washingtonpost.com/opinions/we-need-to-hack-proof-our-elections-an-old-technology-can-help/2018/02/14/27a805bc-0c4b-11e8-95a5-c396801049ef_story.html?utm_term=.bfeb06fa4a86.

Funding elections should be a shared responsibility at the local, state, and federal level, but only Congress has the power to ensure that responsibility is shared by providing grants that must be matched by state and local governments. Obvious first steps for such money should include the items touched on in my testimony today, including replacing paperless voting machines before 2020 and conducting robust post-election audits.

Congress should also share in longer-term funding for things like regular risk assessments and necessary repairs and upgrades for critical infrastructure, as well as grants for cybersecurity resources that are directed to local election offices, which are frequently under-resourced relative to their state counterparts.

Finally, Congress should consider what additional steps it can take to protect our election infrastructure from attacks against private election system vendors, who were targeted in 2016 and are likely to be targeted again. Private companies perform every duty from building and maintaining election websites that help voters determine how to register and where they can vote, to printing and designing ballots, to programming voting machines before each election, to building and maintaining voter registration databases, voting machines, and electronic pollbooks. To be sure, not every jurisdiction outsources all these functions, but all rely on private vendors for some of this work and many for all of it.

And yet, in contrast to other sectors, particularly those that the federal government has designated "critical infrastructure," there is almost no federal oversight of private vendors that design and maintain the systems that allow us to determine who can vote, how they vote, what voters see when they cast their vote, how votes are counted and how those vote totals are communicated to the public. In fact, there are more federal regulations for ballpoint pens and magic markers than there are for voting systems and other parts of our federal election infrastructure.[48]

One important step would be to mandate that vendors report any cyber security incident they discover to both the federal authorities as well as state and local customers. Reporting of cyber security incidents for election vendors may seem like a small step, but it will have a large impact on the overall security position of election officials around the country. Election vendors have stated that such requirements are unnecessary and burdensome and that they are somehow different from the vendors in other critical infrastructure sectors. This is simply not true. We know that the lack of transparency in vendor security is a significant vulnerability to election security. In fact, reporting requirements for cyber security incidents are a bare minimum, and we should be considering additional requirements such as vendor employee background checks and other lessons learned from other critical infrastructure sectors.[49] The Brennan Center has documented some of the additional reasons for mandating such reporting in the 2010 report, *Voting System Failures: A Database Solution*.[50]

---

[48] Compare, for example, 16 C.F.R. §§ 1500.14, 1500.48, 1500.83, 1700.14, with 11 CFR §§ 9405.1 et seq.

[49] Brian Calkin, Kelvin Coleman, Brian de Vallance, Thomas Duffy, Curtis Dukes, Mike Garcia, John Gilligan, Paul Harrington, Caroline Hymel, Philippe Langlois, Adam Montville, Tony Sager, Ben Spear, Roisin, *A Handbook for Elections Infrastructure Security*, Center for Internet Security, February 2018, https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf.

[50] Lawrence Norden, *Voting System Failures: A Database Solution*, Brennan Center for Justice, 2010, https://www.brennancenter.org/publication/voting-system-failures-database-solution.

D. Conclusion

America has made great progress since 2016 in securing our elections. But in an era when hostile nation powers are likely to continue to see American election infrastructure as a target, we cannot rest on our laurels. As one election official noted in an interview with the Brennan Center, "we are trying to build the [protective] wall faster than our opponents are tearing it down."[51] Doing so requires consistent, coordinated resources and leadership from all levels, including Congress, federal agencies, the states, and local governments.

[51] Kathy Boockvar (Acting Secretary of the Commonwealth, Pennsylvania), interview by Brennan Center for Justice, May 3, 2019.

The CHAIRPERSON. Thank you very much.
Ms. Schneider.

STATEMENT OF MARIAN SCHNEIDER

Ms. SCHNEIDER. Chairperson Lofgren, Ranking Member Davis, and Members of the committee, thank you so much for the invitation to testify here today. My name is Marian Schneider, and I am the President of Verified Voting, a nonprofit, nonpartisan organization. Verified Voting's mission is to strengthen democracy for all voters by promoting the responsible use of technology in elections.

We are here today to talk about bolstering election security. Ninety-nine percent of the votes cast in this country are counted by computers, and election administration depends on computers throughout the process. 2016 demonstrated what many of us in this space have long believed, that the threat to our computerized voting systems was not merely theoretical but real and persistent. We must, as a Nation, adopt clear solutions that will change the destructive narrative that election hacking can alter election outcomes.

In our written testimony, we describe threats and solutions for the larger election ecosystems. For voting systems, however, the clear solution is to replace aging and vulnerable voting machines with systems that use a voter-marked paper ballot. Voters mark the paper either with a pen or a computer ballot marking device with assistive features for voters who need them, creating a verifiable record. Then the ballot is scanned and retained in a secure ballot box.

We leverage the computer speed to count ballots quickly, but it is imperative to check that the computer has counted the ballots properly. In the best-practice scenario, as Mr. Norden mentioned, we can check election outcomes by auditing, selecting a random sample of ballots to check the reported results and gather sufficient evidence that the outcome is correct.

While there are different types of auditing, Verified Voting and other experts urge widespread adoption of risk-limiting audits as the most efficient and reliable way of checking the election results. Such audits have a predetermined large chance of leading to a full hand recount if the reported results were incorrect, thus limiting the risk that a wrong outcome will stand.

Verified Voting board members and staff have been involved with every stage of RLA development, from its inception to working with election officials, other groups, and several States to pilot risk-limiting audits.

From 2015 to 2017, I served as Deputy Secretary for Elections Administration in the Pennsylvania Department of State, overseeing both elections and information technology. I have firsthand experience trying to strengthen the cybersecurity of election infrastructure in advance of a Presidential election. I drafted directives for counties to harden their systems, strengthen voter registration database backup protocols, invited the Department of Homeland Security to conduct penetration testing, and initiated a disaster recovery plan for a statewide, election-night-return website. And I worked with heroic, local election officials trying to keep up with the changing threat environment with next to no resources. From

that experience, I urge Congress to support State and local jurisdictions by providing immediate and sustained investment in the security of our elections.

The consensus among the intelligence community is that future attacks on American elections are inevitable. This is a given. It is not whether a system will be attacked but when. Safeguarding systems requires that we assume such breaches will occur or have already. The best practice demands a multilayered approach built around the concept of resiliency. Election systems are resilient if jurisdictions can monitor, detect, and recover from either an intentional attack or a programming error. Resilient voting systems are those that use voter-marked paper ballots, coupled with the risk-limiting audits. Paper ballots and audits are the disaster recovery plan for our voting systems.

A significant number of States have moved toward paper-based systems over the years. Verified Voting tracks this movement on its website and so that is a general recognition of the best practices that we are talking about today. The main barrier to the remaining States is the cost. We call on Congress for the financial investment for jurisdictions to replace aging and vulnerable voting systems, to fund technical and material support to conduct risk-limiting audits, and to fund enhanced security measures for all aspects of election infrastructure.

We also urge investment in the research needed to build better election systems, using open-source software and research into the best methods to ensure voters check their choices before casting their ballots and research that marries security with more universally useable and accessible systems.

Our Nation's election infrastructure is vitally important to our democracy. We must continue the progress begun in the last two years to ensure that our election systems and voting processes are resilient in the face of attack or disaster. With support from Congress, the goal is in reach. Thank you.

[The statement of Ms. Schneider follows:]

Written Testimony of Verified Voting.org
Marian K. Schneider, President

United States House Committee on House Administration
hearing on "Election Security."

May 8, 2019

10:00 a.m. 1310 Longworth House Office Building, Washington, DC

Chair Lofgren, Ranking Member Davis and members of the Committee, thank you for the invitation to submit testimony to the Committee on House Administration hearing on "Election Security." We urge the Committee to move expeditiously to support state and local jurisdictions in strengthening their election systems and provide upfront and sustained investment in election infrastructure and security. Since 2016, it is clear that the threat to our democratic institution of voting is not theoretical, but real and persistent. We must, as a nation, adopt the clear solutions that will allow us to defuse the destructive narrative of election hacking that undermines the very fabric of our democracy.

About Verified Voting

Verified Voting's mission is to strengthen democracy by promoting the responsible use of technology in elections. Since our founding in 2004 by Stanford computer science professor David Dill, we have acted on the belief that the integrity and strength of our democracy relies on citizens' trust that each vote is counted as cast. We bring together policymakers and officials who are designing and implementing voting-related legislation and regulations with technology experts who comprehend the risks associated with election technology. We have provided direct assistance to election officials in implementing the most efficient post-election audits to verify election results. Additionally, we connect advocates and researchers, the media and the public to provide greater understanding of these complex issues.

Our board of directors and board of advisors include some of the top computer scientists, cyber security experts and statisticians working in the election administration arena as well as former and current elections officials. Verified Voting has no financial interest in the type of equipment used. Our goal is for every jurisdiction in the United States to have secure and verifiable elections.

In addition to our expertise and reputation in the field, Verified Voting has assets developed over years of monitoring election administration practice. These include the most complete, accurate and up-to-date publicly-accessible database of voting and tabulation systems in use, and comprehensive archives of news and publications on election technology. Our dataset on voting equipment is used and relied upon by organizations in need of reliable historical and current data on the election equipment. Further, we assist researchers, the press and the public by providing custom datasets for their use.

The Scope of the Problems with Election Security and Current Election Infrastructure

Election administration depends on computers at multiple points in the election process. Equipment for *voting* is but one part of a broad array of election technology infrastructure that supports the conduct of elections today. Some of that technology infrastructure includes voter registration databases, internet facing applications such as online voter registration and polling place lookup, network connections between state government and local jurisdictions, the computers that program the voting devices that record and count votes in addition to the voting devices themselves. Some jurisdictions also use electronic poll books to check voters in at polling sites and most states and localities report election night returns via a website.

To the extent that any of these can be compromised or manipulated, can contain errors, or can fail to operate correctly—or at all—this can potentially affect the vote. Election system security requires not only efforts to prevent breaches and malfunctions, but also fail-safes that address breaches and malfunctions that do occur.

The security of election infrastructure has taken on increased significance in the aftermath of the 2016 election cycle. During the 2016 election cycle, a nation-state conducted systematic, coordinated attacks on America's election infrastructure, with the apparent aim of disrupting the election and undermining faith in America's democratic institutions. Intelligence reports and recent investigations demonstrate that state databases and third-party vendors not only were targeted for attack, but were breached.[1]

The consensus among the intelligence community is that future attacks on American elections are inevitable.[2] The inevitability of attacks is a key concept in cyber security: it's not whether a system will be attacked, but when. Moreover, cyber security experts now agree that it is impossible to thwart all attacks on computer systems. Rather, best practice demands a multi-layered approach built around the concept of resiliency. Systems are resilient if owners can monitor, detect, respond and recover from either an intentional attack or a programming mistake or error. The capacity to recover from even a successful attack is integral to the security of U.S. elections.

Despite considerable progress in the last few years, much work must be done to secure our nation's elections infrastructure. Two primary areas that require immediate and sustained attention are 1) securing both the state and county networks, databases and data transmission infrastructure that touch elections; and 2) instilling confidence in election outcomes by replacing

[1] "Illinois election officials say hack yielded information on 200,000 voters," *Chicago Tribune,* Aug. 29, 2016, http://www.chicagotribune.com/news/local/politics/ct-illinois-state-board-of-elections-hack-update-met-0830-20160829-story.html; "Russian hackers targeted Arizona election system," *The Washington Post,* Aug. 29, 2016, https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html?utm_term=.de487f1d4b90.

[2] *Assessing Russian Activities and Intentions in Recent U.S. Elections*, ICA 2017-01D, Office of the Director of National Intelligence, 2017 at iii; *Securing Elections from Foreign Interference,* Brennan Center for Justice, June 29, 2017 at 4.

older, vulnerable legacy voting systems with new systems that permit reliable recounts and post-election audits.

Voting System Infrastructure Risks

Two basic kinds of electronic voting systems are used in the United States: Direct recording electronic (DRE) and optical scan systems. Both types of systems are computers, and both are prepared in similar ways. The primary difference is that an optical scan system incorporates a voter-marked paper ballot, marked either with a pen or pencil or with a ballot marking device and that ballot is retained for recounts or audits. Optical scan systems leverage the speed of the computer to report unofficial results quickly. The paper ballots provide a trustworthy record of voter intent and allow jurisdictions to monitor their system for problems, detect any problems, (either hacking or error), respond to them and recover by, if necessary, hand counting the paper ballots.

Direct recording electronic (DRE) systems directly record the voter's choices to computer memory. The voter may interface with the voting machine in one of several ways, such as a touchscreen or push buttons, but the voter's selections are recorded directly to memory stored in the machine. There is no software-independent[3] record of voter intent provided with a DRE system. In some states, the DRE systems produce a contemporaneous printout of the voter's choices known as a "voter verifiable paper audit trail" (VVPAT). That paper output cannot be handled by the voter, is usually viewed through a plastic window and may or may not be checked before the voter's choices are directly recorded onto computer memory. There is a risk that the choices saved onto the memory and tabulated may not match the paper record; alternatively, the paper record may not correctly reflect the voter's choices and the voter may not notice the error.

Because DRE systems lack a paper ballot that was separately marked by the voter and tabulated separately, errors or malware on the software could result in an undetectable change in the election outcome. Replacing DREs is urgent because, by design, it is impossible to verify that the computer correctly captured the voter's choices. Even those with VVPAT present security risks and verification challenges that are difficult to overcome.[4] A printout of election results

[3] Software independence in voting systems was described by Ron Rivest (MIT) and John Wack (NIST) as follows: "*A voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome.*" *See* Rivest, R. and Wack, J. "On the Notion of Software Independence in Voting Systems." Available at https://people.csail.mit.edu/rivest/RivestWackOnTheNotionOfSoftwareIndependenceInVotingSystems.pdf

[4] The committee may have heard that the precinct voting devices are "unhackable." That statement is untrue. Each precinct voting device is programmed by a regular laptop or desktop computer. The program files are then loaded onto the precinct voting device via some kind of memory card, cartridge or USB stick. This is true for every kind of computer that counts votes. An error or malware on the computer that programs the voting devices could infect the entire county. If that computer is connected to a network (which is not a best practice but may occur anyway), a phishing attack, for example, in which the attacker obtained login credentials could provide a pathway for the attacker to modify the ballot definition file. Alex Halderman, Professor of Computer Science at the University of Michigan, has demonstrated numerous times how this could be done, including in the *New York Times* video available here: https://www.nytimes.com/2018/04/05/opinion/election-voting-machine-hacking-russians.html

from the memory card of a DRE after the fact or a printout of "cast vote records" does not provide any additional verification of the election results. Those printouts simply call up the data that is stored on the computer's memory. If the data was not stored correctly, whether because of malware or malfunction in the voting system, a printout of incorrect data is meaningless. Without a contemporaneous software independent record of voter intent, there is no way to verify, audit or recount DREs.

Mitigating Voting System Risks

Fortunately, for voting systems, a general consensus has formed on the steps necessary to provide a secure, reliable and verifiable election:

- A paper ballot (marked by pen or computerized ballot marking device) that voters can verify before casting;
- Routine, robust post-election audits to either confirm that reported outcomes are accurate or identify problems for further investigation before vote counts are finalized; and
- The ability to carry out full manual recounts if needed.

For technology used for marking and counting votes, voters must be able to confirm first-hand that their ballots were indeed marked as they intended, and election officials must be able to use those ballots to demonstrate that all the votes were included and were counted as cast. This process is crucial to defuse the narrative that our elections can be hacked.

This bridge between the voter and correctly reported outcomes requires a physical artifact as evidence of the voter's intent, and a process for checking. That artifact is typically the **paper ballot** that is voter-marked, either with a pen or pencil or through the use of an accessible interface such as a ballot marking device. An inferior alternative, to be replaced as soon as possible, is the "Voter-Verifiable Paper Audit Trail" provided by some DRE machines. Whatever the physical record, it must have been available to the voter for his or her review prior to casting in order to serve as a record of voter intent. Voting systems, especially ballot marking devices, should make it as easy as possible for voters to verify their ballots.

Post-election tabulation audits provide the crucial check of vote counts against voters' ballots. It is important to check the ballots themselves, not relying upon software-generated images or other artifacts that voters themselves could not verify. Effective audits manually inspect enough of the voter-verified paper ballots to provide strong evidence that the reported election outcomes match the ballots. The most robust tabulation audits, called **risk-limiting audits**, provide a large, statistically guaranteed minimum chance of correcting outcomes that are wrong due to tabulation errors. Colorado and Rhode Island have passed laws to require risk-limiting audits before election results are certified. Many other states require some weaker form of tabulation audit, which may or may not provide evidence that outcomes are correct -- and, in some states, is conducted too late to correct wrong outcomes.

Tabulation audits do not stand alone. Other compliance procedures ensure that all ballots are accounted for and the numbers of ballots cast reconciles with the number of voters who signed in, and that important chain of custody security procedures have been followed each

election. Put together, these practices provide assurance that voters' ballots determine the election results. Other election processes also should be routinely audited.

Full manual recounts must be available, when necessary, to correct election outcomes. Risk-limiting audits, by definition, require full manual recounts when audit samples do not find strong evidence that the reported outcome is correct. The best recount provisions allow for full recounts of elections with very close margins, and for full or partial recounts at candidate expense (unless errors are found) in other contests, all conducted by hand. Many recount laws allow ballots to be re-tabulated by machine, inherently a poor response to cybersecurity concerns.

Consensus Support for Change

The chorus of voices calling for the security measure of voter marked paper ballots has grown louder since 2016. On September 17, 2018, a federal court in Georgia issued a decision in *Curling v. Kemp* finding that the persistent vulnerabilities in the Georgia's paperless voting system raised profound constitutional issues that require urgent action from state officials. In explaining its ruling, the court outlined the constitutional imperative to secure election systems against modern cyberthreats, thus protecting voters' due process and equal protection rights.

The Georgia court's conclusion underscores the stakes associated with ensuring secure and reliable election systems: "The 2020 elections are around the corner. If a new balloting system is to be launched in Georgia in an effective manner, it should address democracy's critical need for transparent, fair, accurate, and verifiable election processes that guarantee each citizen's fundamental right to cast an accountable vote."[5]

In September 2018, the National Academies of Science, Engineering and Medicine issued a Consensus Report that, among other recommendations, emphasizes the importance of paper ballots and post-election audits.[6]:

> 4.11 Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine (using a ballot-marking device); they may be counted by hand or by machine (using an optical scanner). Recounts and audits should be conducted by human inspection of the human-readable portion of the paper ballots. Voting machines that do not provide the capacity for independent auditing (e.g., machines that do not produce a voter-verifiable paper audit trail) should be removed from service as soon as possible.

[5] *Curling v. Kemp*, No.1:17-CV-02589-AT, at 46

[6] National Academies of Science, Engineering, and Medicine, 2018, *Securing the Vote: Protecting American Democracy*, available for download at https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy.

5.6 Jurisdictions should conduct audits of voting technology and processes (for voter registration, ballot preparation, voting, election reporting, etc.) after each election....

5.7 Audits of election outcomes should include manual examination of statistically appropriate samples of paper ballots cast.

5.8 States should mandate risk-limiting audits prior to the certification of election results.... [When fully implemented, risk]-limiting audits should be conducted for all federal and state election contests, and for local contests where feasible.[7]

The Committee also analyzed and detailed the cyber security threats that exist for electronic voting systems and other election systems. Key findings on cyber security include:

- all digital information—such as ballot definitions, voter choice records, vote tallies, or voter registration lists—is subject to malicious alteration;
- there is no technical mechanism currently available that can ensure that a computer application—such as one used to record or count votes—will produce accurate results;
- testing alone cannot ensure that systems have not been compromised; and
- any computer system used for elections—such as a voting machine or e-pollbook—can be rendered inoperable.[8]

Ongoing Improvements

Many savvy election officials throughout the country, at state and local levels, have always taken election security seriously, but after breaches of voter-registration sites were initially reported in mid-2016 the subject has risen to a top-level priority nationally. At many conferences for state and local election officials, security now is a topic of keynotes and workshops, and at some conferences has dominated the discussion. Speaking for myself, as the Deputy Secretary for Elections and Administration in Pennsylvania in 2016 and later as Special Advisor to Governor Tom Wolf on Election Policy, we implemented several steps in the runup to the 2016 election to protect election infrastructure, including issuing guidance to counties about implementing best practices to harden their voting systems, engaging with the United States Department of Homeland Security to conduct penetration testing and assessment of the PA Department of State's networks, engaging a security firm to also conduct penetration testing of those networks, evaluating and strengthening the voter registration database backup protocol, and planning for attacks on the Election Night Return website to foil any attempts to undermine it.

Election administration is generally run at the local level, complicating coordinated efforts to bolster election security. Approximately 8,000 jurisdictions administer elections in the United States, and many of those are small county or municipal government entities that serve a

[7] *Securing the Vote* at 7-9.

[8] *Id.* at 90

few voters.[9] This decentralized structure causes variability in both election administration processes and cyber security readiness. While some view this decentralization as protective, the existence of such variability in resources can actually be more problematic as attackers seek to attack the weakest link. The existence of such variability in processes, equipment and best practices underscores the need for enough funding to reach those local jurisdictions.

Beginning in 2017, federal, state and local governments have engaged in concerted efforts to improve election cybersecurity. First, in January, 2017, the Department of Homeland Security designated elections as critical infrastructure. As a result, the Elections Infrastructure-Information Sharing Analysis Center (EI-ISAC) was created to provide information sharing and resources to states and localities involved in elections. Additional work on information sharing and dissemination of best practices occurs through the Elections Government Sector Coordinating Council established in October, 2017. Similarly, a private sector counterpart made up primarily of voting system vendors also works towards the information sharing goal.

Election officials in at least 36 states have engaged with the Center for Internet Security to place network monitoring services on their networks. Moreover, several organizations have researched and published guidelines for securing election computer assets, mostly focused on networks and network connected components.[10] Federal agencies including the Election Assistance Commission and the Department of Homeland Security, among others, have been working to disseminate this information as widely as possible.

On the voting system front, in 2016, 70% of voters voted on systems that had some kind of paper record. Currently, more voters, approximately 77% will likely vote on systems that have a paper record in 2020. Since March 2018, the states with the most vulnerable unverifiable equipment have made progress in moving towards replacing those systems. For example, Delaware plans to deploy new ballot marking devices for all voters and Georgia passed legislation appropriating the funding for new voting systems. Pennsylvania has directed all counties to replace their voting systems by the 2020 primary and all new systems must have a voter-marked paper ballot. Louisiana and South Carolina still use 100% paperless DRE systems, and in another 8 states, a significant number of voters still use paperless DRE systems as their primary voting method.[11]

---

[9] Kimball, D., Baybeck, B. "Are all Jurisdictions Equal? Size Disparity in Election Administration," *Election Law Journal,* Vol. 12, No. 2 at 131.

[10] *See, e.g.* Securing Voter Registration Data" National Protections and Programs Directorate, Department of Homeland Security, June 26, 2018 Retrieved from:https://www.dhs.gov/sites/default/files/publications/Securing%20Voter%20Registration%20Data_0.pdf; "A Handbook for Elections Infrastructure Security, Version 1.0." the Center for Internet Security, February 2018, Retrieved from: https://www.cisecurity.org/elections-resources/; "The State and Local Election Cybersecurity Playbook," Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2018. Retrieved from: https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#practices. The extent to which jurisdictions adhere to these recommendations will determine the level of integrity they are perceived to have.

[11] Arkansas, Indiana, Kansas, Kentucky, Mississippi, New Jersey, Tennessee and Texas.

Only three states conduct routine, mandatory robust post-election audits and the remaining states vary widely in the effectiveness of post-election audit processes. Many states have worked to improve their post-election audits, either by strengthening their existing audit requirements or by moving toward implementation of risk-limiting audits. For the first time in 2018, Wisconsin conducted its mandatory post-election audits (which are not risk-limiting) before the final results were certified. Six states currently provide, in statute or rule, for mandatory or optional risk-limiting audits (RLAs), and several states are presently considering new RLA requirements. At least seven states have conducted pilot risk-limiting audits. Verified Voting has provided advice to legislators and others seeking to improve their states' audit requirements. We, along with other organizations, also provided crucial technical assistance in the first pilot RLAs in Virginia (conducted by the City of Fairfax in cooperation with state officials) and Rhode Island (conducted by the state board of elections in cooperation with local officials). These and other pilots have helped to model not only best election practices, but broad collaboration to address a national threat.

Although all of the steps that have occurred since 2016 are useful, and long overdue, it's clear that more work needs to be done. Historically, elections and election infrastructure have been woefully underfunded, and more resources are necessary to properly equip local jurisdictions to manage and lessen the risks associated with computerized voting.

Preparations for 2020 and Recommendations

Our discussion above has highlighted the steps necessary to secure our elections. To prepare for 2020, those best practices must be adopted more widely by as many jurisdictions as possible. For that to occur, adequate financial investment in cyber security best practices, replacement equipment and post-election audit processes needs to occur immediately and continue at a sustainable level moving forward.

Adoption of voting systems with voter marked paper ballots and risk-limiting audits would certainly be an important goal in advance of the 2020 election. We note, however, that some of the commercially available ballot marking devices sold today present some risk that voters will not intentionally verify that the device correctly captured their choices. The lack of intentional verification can weaken the effectiveness of a post-election audit as a tool to verify election outcomes. In the short term, in jurisdictions that have purchased ballot marking devices intended for use by all voters, we strongly urge an evaluation of voting processes to incorporate a separate step that reduces the risk that voters will neglect to verify their choices.

Equally important is the need for research into voters' verification of their ballots is funding to support science-based improvements to secure systems in the public interest. That research should endeavor to balance security and accessibility needs and reduce the tension between these two principles.

We see an urgent and ongoing need for investment to bolster national election security for 2020 and beyond. Here we briefly state some of the important focus areas:

- Unverifiable Direct Recording Electronic voting systems should be replaced with voter-verifiable systems with paper ballots as soon as possible. The replacement systems should make it as easy as possible for voters to verify their ballots and for officials to audit the tabulation.
- Rigorous post-election audits, preferably risk-limiting audits, should be adopted as soon as feasible, prioritizing federal and statewide contests. Such audits are possible wherever voter-marked paper ballots are used, Both technical and material support is needed to conduct these audits and by implication, increased funding.
- Funding to support audits and where necessary recounts of close contests in the nature of "recount insurance" when close contests require more scrutiny.
- Jurisdictions that have purchased ballot marking devices intended for use by all voters should urge voters to verify their ballots before casting, and should adopt procedures that support voters in verification. Current ballot marking devices raise concerns that voters will fail to check their ballots, undermining the ballots' value as evidence of voter intent.
- Research is needed into how effectively voters verify their ballots -- especially ballots printed by ballot marking devices – and how to enhance voter verification. This research should proceed in tandem with other usability research to ensure that all voters can vote independently and accurately.
- Continued investment in securing all aspects of election infrastructure – at all levels – from cyber attack remains essential. Voter registration databases, electronic pollbooks, voting systems and election reporting systems are among the targets that must be protected.
- Any legislation with funding should include the following:
    - Incentives for development of open source voting systems
    - Incentives for development of open source software to assist jurisdictions with implementing risk-limiting audits
    - Prohibition on direct recording electronic voting systems.
    - Prohibition on return of voted materials via the internet or mobile phone
    - Incentives for legal public testing of election systems to identify possible security vulnerabilities before systems are deployed in the field.
- Congress should consider expanding testing or certification requirements for election systems that do not specifically tabulate ballots. For example, electronic poll books are widely used but no federal oversight or testing occurs. In the short term, we recommend some method of examining those systems to identify key issues for correction before deployment.

Our nation's elections infrastructure is vitally important to our democracy. We must continue the progress that has begun in the last two years to ensure that our election systems and voting processes are resilient in the face of attack or disaster. With additional resources from Congress, the goal is within our reach.

The CHAIRPERSON. Thank you very much.
Mr. Hall.

STATEMENT OF JOSEPH LORENZO HALL

Mr. HALL. Chairperson Lofgren, Ranking Member Davis, and Members of the Committee, thank you for the opportunity to speak with you today. My name is Joseph Lorenzo Hall. I am the Chief Technologist at the Center for Democracy and Technology. For 25 years, CDT has been a leader in protecting digital civil liberties and democratic principles online. My Ph.D. work at UC Berkeley focused on voting machines, and I have served on a number of State-level independent reviews of voting systems. Today I will talk first about what we saw in 2018, and then CDT's five priorities for election security as we head into 2020.

While 2018 did not see the cybersecurity attacks on election systems that we saw in 2016, a number of attacks did target campaigns and campaign infrastructure. The midterms were just not a juicy target for attackers, at least not as attractive as 2016 or 2020 election cycles. The issues we did see with election systems in 2018 involved isolated but systemic issues more easily explained as failures rather than attacks.

For example, in Johnson County, Indiana, a misconfigured computer server caused electronic pollbooks to crash across the entire county. No one could vote for four hours. In a case of election dēējáa vu, a serious ballot design flaw likely contributed to tens of thousands of missing votes in a Florida U.S. Senate contest. We were in many ways lucky and thankful that we didn't see attacks like those of 2016, but we still have a long way to go in terms of hardening elections.

CDT believes the following five priorities are crucial going into 2020: First, Congress must prioritize the replacement of dangerously outdated voting technologies. We learned after the Help America Vote Act of 2002 that elections are one area of civic life that we cannot fully digitize. To enable meaningful recounts and post-election audits, we must have software-independent, voter-verifiable paper records. Very simply, it is time for a paper mandate in elections for Federal office. Or at least some very attractive incentives designed to replace paperless systems.

Second, Congress should limit the use of paperless remote voting systems. There are some contexts, such as uniformed and overseas voting, where jurisdictions allow email, fax, or even internet voting, occasionally disguised as remote ballot-marking systems. These systems do not have a paper record backing up those votes, and they may even expose jurisdictions to increased risks of cyberattack. Rather than allowing, for example, any absentee voter to use these systems as some jurisdictions do, paperless remote voting should be limited to only those who could not otherwise vote in another manner.

Third, Congress should promote the research, development, and implementation of risk-limiting audits. Yes, that is a wonky term, risk-limiting audits, but you can think of them as low-cost recounts. In a risk-limiting audit, paper ballots are randomly selected and compared to their digital equivalent until there is enough evidence that, if you did a full recount of those paper records, you

would know that the outcome of the race wouldn't change. And as mentioned, only a few States currently permit these kinds of audits, are engaged in pilot projects, and to encourage more, Congress should provide incentives for two things: research and development to make them more precise and useable, and then pilot projects with published reports which would greatly help others along this journey.

Fourth, Congress should commit to long-term funding of the U.S. election infrastructure. The ongoing evolution of election administration desperately needs a stable and long-term source of funding. Without this, elections will continue to be threadbare and a natural target for attackers that want to affect our economy, our society, and our democracy. The down payment in ongoing funding contemplated in the Election Security Act, now part of H.R. 1, is a good start.

Finally, Congress must increase the budget of the U.S. Election Assistance Commission. The EAC now has a full complement of sitting Commissioners. It is preparing right now—preparing election officials and voting system testing for 2020, and it is in the process of finalizing version 2.0 of the Federal voting system standards, the VVSG. It is a very busy time for the EAC right now. The last time there was this level of activity at the EAC was in 2010 when its budget was roughly twice what it is now.

In summary, replace paperless voting systems, incentivize risk-limiting audits, and fund election infrastructure and security. Thank you very much.

[The statement of Mr. Hall follows:]

Testimony of

Dr. Joseph Lorenzo Hall
Chief Technologist
The Center for Democracy & Technology[1]

Hearing on "Election Security"
The Committee on House Administration, U.S. House of Representatives

May 8, 2019

Chairwoman Lofgren, Ranking Member Davis, and members of the Committee:

Thank you for the opportunity to speak to you today and to submit these written remarks on one of the most critical subjects facing our democracy today, election security.

My name is Joseph Lorenzo Hall,[2] I'm the Chief Technologist at the Center for Democracy & Technology (CDT). For almost twenty-five years, CDT has been a leader in protecting digital civil liberties and defending democratic principles online. With multidisciplinary programs focused on free expression, privacy and data, an open internet, security and surveillance, and internet architecture, CDT provides a complete and collaborative approach to identifying practical solutions and policy recommendations for today's most difficult technology questions.

I oversee CDT's Election Security and Privacy project, which focuses on educating the elections community about cybersecurity concepts and practices through a set of online interactive courses, "Election Cybersecurity 101" field guides, and by holding regular briefings and trainings for election officials, legislative staff, and journalists. I hold a PhD and Masters degrees from the University of California, Berkeley in information science and astrophysics; my PhD dissertation work involved studying electronic voting systems as a critical case study in the transparency of black box technologies used by governments as they increasingly adopt digital technologies.

---

[1] The Center for Democracy & Technology (CDT) is a nonpartisan nonprofit public interest advocacy organization that works to advance human rights online, and is committed to finding forward-looking and technically sound solutions to the most pressing challenges facing users of electronic communication technologies. With expertise in law, technology, and policy, CDT promotes policies that protect and respect users' fundamental rights to privacy and freedom of expression, and enhance their ability to use communications technologies in empowering ways. CDT has testified in front of Congress numerous times in its over 25-year history and is a highly trusted voice in technology policy. I would like to thank CDT staff and especially Senior Technologist Maurice Turner for assistance with preparing this testimony. Please direct additional inquiries to me via email (joe@cdt.org) or phone (+1-202-407-8825).

[2] My curriculum vitae is here: https://josephhall.org/HallJosephResume.pdf.

1. Securing Elections is a Systems Problem

The events leading up to the 2016 election were a wake-up call for the entire elections community.[3] Nation-state adversaries that attacked electoral and campaign systems were proof that powerful adversaries sought to sabotage the very machinery of our democracy,[4] and that election officials must harden their defenses and prepare for inevitable future attacks.

After 2016, election administrators had to adapt to address cybersecurity threats from well-resourced nation-state attackers trained to scan and compromise election information systems. Security concerns around election technologies up to this point had focused on voting machines themselves – the machines used in polling places to cast votes. However, the lesson of the 2016 election attacks was that technology is now an integral part of the elections, campaign, and voting processes, such that any subsystem that connects to the elections systems is a target for malicious attacks. While certainly the security of vote-casting systems deserves ongoing attention, we must increasingly reinforce the security of the entire system that goes into running modern elections, across different functions like voter registration, vote-casting, vote tabulation, and election-night reporting. This involves different types of information systems such as voting machines, voter registration systems, electronic pollbooks, county and state information networks, and the back-office business networks used by election administrators, their staff, and volunteers.

In short, the election community learned from 2016 that election security is a *systems* problem and that the threats and risks involved are best dealt with by using systems-level solutions, such as designs and mitigations that can neutralize entire classes of attacks (e.g., multi-factor authentication).

For election administrators, their staff, and volunteers, this is a time of cultural change, where the security of the election system now equals the importance of other legal, logistical, and performance goals. Elections workers are now in the spotlight of international cybersecurity attention, and they've had to learn new tactics and strategies to reduce risks to and increase resiliency of election systems and processes.

2. Progress Since 2016 Has Been Encouraging

Compared to 2016, cyberattacks against elections interests in 2018 were relatively quiet, directed more towards campaign entities rather than election administrators. Three Congressional campaigns[5]

---

[3] United States Director of National Intelligence, "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections," (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[4] National Academies of Sciences, Engineering, and Medicine. 2018. *Securing the Vote: Protecting American Democracy.* Washington, DC: The National Academies Press. https://doi.org/10.17226/25120; Lawrence Norden and Wilfred U. Codrington III, "America's Voting Machines at Risk – An Update," Brennan Center for Justice (Mar. 8, 2018), https://www.brennancenter.org/analysis/americas-voting-machines-risk-an-update.

[5] Olivia Beavers, "Primary season cyberattacks illuminate campaign vulnerabilities," *The Hill* (Oct. 7, 2018), https://thehill.com/policy/cybersecurity/410229-primary-season-cyberattacks-illuminate-campaign-vulnerabilities.

were targeted with tactics from malicious keylogging software,[6] phishing attacks,[7] brute-force login attempts,[8] and denial-of-service (DoS) attacks.[9] In addition, a 2018 Senate campaign was unsuccessfully targeted by Russian attackers using the same methods that had been successful in 2016.[10] Finally, leading up to and after the 2018 election, there were incidents involving successful attacks on the email system of the National Republican Congressional Committee (NRCC) and a number of malicious websites mimicking the websites of political organizations.[11]

Despite these attacks on campaign-related entities, election administrators did not appear to be heavily targeted in 2018. The level of awareness about cybersecurity was high throughout the election community, and there were dozens of opportunities for stakeholders (election officials, journalists, and legislative staff) to attend briefings, trainings, and continuing cybersecurity education designed specifically for election officials.[12] Many of these efforts prioritized basic cybersecurity concepts that had been problematic in the 2016 elections. These included issues such as good password hygiene,[13] two-factor login (or two-step login),[14] and mitigation of distributed DoS attacks.[15] While in some cases this outreach has included hundreds of election officials at a time, given that there are more than 8,000 election jurisdictions around the country, these educational efforts will need to be sustained and adapted in time to new technologies and techniques.

Unfortunately, in addition to malicious attacks, errors and flaws in election operations remain a significant issue. In the 2018 general election there were serious breakdowns across all polling places in a small number of jurisdictions, most notably in New York City where jammed optical-scanning

---

[6] Keylogging software is malicious software that is designed to record and send everything a victim types into a keyboard.
[7] Phishing attacks involve spoofed email that convinces the victim to click on a link or email attachment to install malicious software or to disclose private information to an attacker.
[8] Brute-force login attempts involve an attacker quickly and repeatedly guessing many different combinations of usernames and passwords in order to gain unauthorized access to an information system.
[9] A denial-of-service (DoS) attack is any kind of attack that results in an service no longer functioning as it normally would, usually achieved by directing enormous amounts of network traffic to the victim computer causing it to have no capacity to respond to legitimate traffic. In a distributed denial-of-service (DDoS) attack, the increased traffic volume comes from a large distribution of sources, making the attack more difficult to stop.
[10] Associated Press, "Democratic Sen. Claire McCaskill confirms Russian hacking attempt," *Los Angeles Times* (Jul. 27, 2018), https://www.latimes.com/politics/la-na-pol-russia-hacking-mccaskill-20180727-story.html.
[11] "2019 Internet Security Threat Report, Volume 24," *Symantec* (February 2019), https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.
[12] Efforts included those of the Belfer Center at Harvard Kennedy School, the Center for Internet Security (CIS), the National Council of State Legislatures (NCSL), the Center for Democracy & Technology (CDT), the Center for Technology & Civic Life (CTCL), the International Association of Government Officials (iGO) as well as US Government agencies such as the Department of Homeland Security (DHS) and the U.S. Election Assistance Commission (EAC).
[13] "Election Cybersecurity 101 Field Guide – Passwords," Center for Democracy & Technology (Aug. 29, 2018), https://cdt.org/insight/election-cybersecurity-101-field-guide-passwords/.
[14] "Election Cybersecurity 101 Field Guide – Two Factor Authentication," Center for Democracy & Technology (Aug. 3, 2018), https://cdt.org/insight/election-cybersecurity-101-field-guide-two-factor-authentication/.
[15] "Election Cybersecurity 101 Field Guide – DDoS Attack Mitigation," Center for Democracy & Technology (Nov. 2, 2018), https://cdt.org/insight/election-cybersecurity-101-field-guide-ddos-attack-mitigation/.

machines caused long lines[16] and in Johnson County, Indiana where failed connections to electronic pollbook databases stopped voting throughout the county for four hours (with no extension of polling hours).[17] Basic ballot design errors remain a serious problem, with a poor ballot design in one U.S. Senate race potentially disenfranchising tens of thousands of voters.[18] These kinds of errors are especially concerning as a clever adversary could attempt to make their attacks appear to be a result of error (and not from intentionally malicious activity). In order to best be able to detect and correct anomalous activity due to malicious attacks, it is important to minimize systemic or potentially outcome-changing flaws with election technology and processes.

3. Election Security Priorities Heading into 2020

CDT believes the following five areas must be policy priorities heading into 2020:

3.1. Prioritize the Replacement of Dangerously Outdated Voting Technologies;
3.2. Limit the Use of Paperless Voting Systems;
3.3. Promote Research, Development, and Implementation of Risk-Limiting Audits;
3.4. Commit to Long-Term Funding of U.S. Election Infrastructure; and,
3.5. Return the EAC Budget to Nominal Levels.

3.1. Prioritize the Replacement of Dangerously Outdated Voting Technologies

While states and local jurisdictions continue to make progress updating their outdated voting technologies with newer systems that keep an auditable voter verifiable paper record,[19] it is important to prioritize the continuing replacement of paperless direct-recording electronic (DRE) systems. DRE systems are not "software-independent" systems,[20] are unauditable, and as such unsuitable for government elections. There are good signs that many of the jurisdictions we worried the most about

---

[16] Ian MacDougall, "What Went Wrong at New York City Polling Places? It Was Something in the Air. Literally." *ProPublica Electionland* (Nov. 6, 2018), https://www.propublica.org/article/new-york-city-polling-places-midterms-2018-humidity.

[17] Voting System Technical Oversight Program, "A Preliminary Investigation of ES&S Electronic Poll Book Issues in Johnson County, Indiana for the 2018 General Election," Indiana Secretary of State (Dec. 31, 2018), https://www.in.gov/sos/elections/files/Report%20-%20Johnson%20County%20ePB%20Investigation%20Dec%2031%202018.pdf (Indiana VSTOP report).

[18] Dana Chisnell and Whitney Quesenbery, "How a badly designed ballot might have swayed the election in Florida," *Washington Post* (Nov. 12, 2018), https://www.washingtonpost.com/outlook/2018/11/12/how-badly-designed-ballot-might-have-swayed-election-florida/.

[19] Marc Levy, "Pennsylvania Senate moves to slow replacing voting machines," *Washington Post* (Apr. 30, 2019), https://www.washingtonpost.com/national/pennsylvania-senate-moves-to-delay-replacing-voting-machines/2019/04/30/b93c7f92-6b88-11e9-bbe7-1c798fb80536_story.html; Mark Niesse, "New Georgia voting machines win final vote in state House," (Mar. 14, 2019), https://www.ajc.com/news/state--regional-govt--politics/new-georgia-voting-machines-win-final-vote-state-house/twQCxrn1Cv9bFbLcUEwTlN/.

[20] "A voting system is software-independent if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome." Ronald L. Rivest and Madars Virza, "Software independence revisited," *Real-World Electronic Voting: Design, Analysis and Deployment*, CRC Press (2016), https://people.csail.mit.edu/rivest/pubs/RV16.pdf.

in 2016 and 2018 – notably, Pennsylvania and Georgia[21] – have committed to move to voting systems with an auditable paper record. However, until there is a federal mandate or a particularly attractive incentive tied to paper-based systems, there will continue to be jurisdictions that use completely electronic (paperless) systems with no auditable record, both because 1) some jurisdictions have already purchased paperless systems in the recent past and have no available resources to purchase new systems, and/or 2) these kinds of systems are unfortunately still available for sale.

3.2. Limit the Use of Paperless Voting Systems

As the state and local jurisdictions continue to modernize their election systems, it is important to also limit the potential risk of malicious attacks or changes to official ballot data through the use of remote vote-casting or ballot-marking systems that do not require a paper record be transmitted to an election official. These forms of paperless remote voting – often used for military and overseas voting, for voters with disabilities, and for voters in hard-to-reach rural areas – can include email, fax, and even internet voting, and must be kept to the minimum number of voters possible, in order to minimize the risks they may pose.[22] These systems 1) unacceptably increase the risk that votes may be changed on the client-side (due to malware on a voter's device), in transit (due to hostile network attackers), or on the server (compromised web or application server) and 2) unacceptably increase the risk that the information systems facilitating remote voting may themselves be subject to attack and potential compromise.[23]

3.3. Promote Research, Development, and Implementation of Risk-Limiting Audits

The secret ballot was a remarkable public policy invention at the turn of the 20th century, reducing the ability to buy votes and exercise undue influence, while paradoxically depressing voter turnout – voters could no longer get paid for their vote.[24] Put differently, the secret ballot was a technical and process development in election administration that resulted in a more trustworthy vote count.

The equivalent to the secret ballot for the 21st century is the risk-limiting post-election audit. Risk-limiting audits provide statistical assurance of the correctness of an electoral outcome by

---

[21] *Id.*, Levy and Niesse, fn. 19.

[22] From a network security perspective, remote ballot-marking systems should only store voted ballot data on the client-side of the communication, not the server-side (the marking interface or software should work without a network connection once activated or downloaded), to prevent transmission of voters' choices over the network; people should be required to send via postal mail or courier if at all possible, rather than transmit an electronic vote and potentially waive their ballot privacy if jurisdictions require ballot duplication for these kinds of remotely cast ballots.

[23] Election systems that must be available over the internet and web – e.g., voter registration systems, election night reporting systems – should be isolated in their own separate network segment (called a network demilitarized zone or network DMZ). This has proved effective at stopping common types of attacks, *see:* Nathaniel Herz, "Hackers broke partway into Alaska's election system in 2016. Officials say no damage was done." *Anchorage Daily News* (May 7, 2018), https://www.adn.com/politics/2018/05/07/hackers-broke-partway-into-alaskas-election-system-in-2016-officials-say-no-damage-was-done/.

[24] Jac C. Heckelman, "The effect of the secret ballot on voter turnout rates," *Public Choice* **82**:1-2, 107-124 (1995); Jac C. Heckelman, "Revisiting the relationship between secret ballots and turnout: A new test of two legal-institutional theories," *American Politics Quarterly* **28**:2, 194-215 (2000), http://users.wfu.edu/heckelic/papers/published/APQ.pdf.

examining a randomly selected subset of ballots.[25] Alternatively, an official can conduct a full manual recount, which by definition is the correct result. A number of states now permit or require risk-limiting post-election audits,[26] and Congress should work to promote increasing experience, development and use of risk-limiting audits through incentives to States and localities in piloting these methods and sharing their experiences. With such a nascent field as risk-limiting post-election auditing, it is also important to encourage additional research and development of new methods and technologies.[27] In addition, incentives could be put to good use to encourage researchers to explore increasingly usable and modular end-to-end cryptographic or "open audit" voting technologies.[28]

3.4. Commit to Long-Term Funding of U.S. Election Infrastructure

There is a long-standing need for a long-term source of funding for elections infrastructure, which has only become more acute now due to increasing cybersecurity risks. Election systems and the systems that support them are critical infrastructure that require sustained and ongoing resources, support, and investment in order to harden their defenses. Funding for election security will help undergird infrastructure at the state and regional level as well as shore up our frontline defenses by ensuring dedicated funds for election security are available to local election officials.

Where funds were absorbed by activities at the state level, some local election officials did not directly benefit from the relatively modest $380 million in 2018 HAVA security funds.[29] With no indication of forthcoming money at the federal level, state-level election administrators may have decided that this money was best spent on state-level infrastructure. A regular cycle of directed election administration funds would allow for both state-level and local-level investment to help local election officials upgrade to more modern and secure information systems and practices.

3.5. Return the EAC Budget to Nominal Levels

The U.S. Election Assistance Commission (EAC) is in desperate need of a significant budget increase in order to meet the tremendous security needs of election officials. The EAC is a critical part of our national election infrastructure, providing a proven mechanism for distribution of modernization

---

[25] Mark Lindeman and Philip B, Stark, "A Gentle Introduction to Risk-limiting Audits," *IEEE Security & Privacy* **10**:5, 42-49 (2012), https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

[26] Including Colorado, Michigan, Rhode Island, and Virginia, *see:* Malachi Barrett, "'Risk-Limiting' Audits Could Provide Election Assurances," *Government Technology* (Dec. 5, 2019), https://www.govtech.com/security/Risk-Limiting-Audits-Could-Provide-Election-Assurances.html.

[27] For example, methods of *precinct-count* single-ballot ballot-comparison risk-limiting audits (ballot-comparison audits are currently only practical on central-count systems), which would allow the most statistical power by counting the smallest number of ballots per contest.

[28] Ben Adida, "Helios: Web-based Open-Audit Voting," *USENIX Security Symposium 2008* (2008), https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf.

[29] Ashley Lopez, "Local Officials Call Federal Election Funds 'A 10-Cent Solution To A $25 Problem'," *NPR News* (Aug. 4, 2018), https://www.npr.org/2018/08/04/634707340/local-officials-call-federal-election-funds-a-10-cent-solution-to-a-25-problem ; Blake Paterson and Ally J. Levine, "Fund Meant to Protect Elections May Be Too Little, Too Late," *ProPublica Electionland* (Aug. 21, 2018), https://www.propublica.org/article/fund-meant-to-protect-elections-may-be-too-little-too-late.

funding, oversight of the voting system testing and certification process, advice and training in election administration, and serving as the steward of the national voting system standards, the Voluntary Voting System Guidelines (VVSG). Approving an updated VVSG is a priority for the EAC[30] and supporting its implementation will be a major undertaking. The last time the EAC had a quorum of four sitting commissioners was in FY 2010 during which their budget was $16.5 million,[31] roughly double its current FY 2019 budget of $9.2 million.[32]

4. Compounded Risks from the Wider Ecosystem

In addition to what was well-known about election cybersecurity attacks in 2016 against voter registration databases and networks that hosted voter registration databases, the recent Mueller Report further implicates two additional types of targets: 1) a voting system services provider, and 2) at least one Florida county, which both had their networks compromised by officers of the Russian GRU (military intelligence).[33] Malicious software of some undisclosed type was installed by the attackers on their networks, allowing attackers to potentially change traffic in transit on the network or break into additional machines connected to the network.

These details are instructive in two ways: first, despite the election community's renewed focus on cybersecurity, other entities contracted to run pieces of elections – e.g., software developers, services vendors, logistics providers, hardware manufacturers, printers – may be compromised by an attacker seeking to influence the election or election operations, allowing a "stepping stone" attack where attackers compromise clients or vendors downstream of their ultimate target. Second, while election defenders rightly focus on hardening election officials' networks, those networks may be connected to other government networks – municipal, county, state – that may themselves be compromised.

The wider ecosystem of election officials' vendors and partners should adhere to generally-accepted cybersecurity practices, which might require a mixture of incentives and regulation. A key piece of a mature cybersecurity practice is a functional vulnerability handling process and associated vulnerability reporting mechanisms, ensuring that vulnerabilities can be properly fixed and establishing a public vulnerability reporting program. Election Systems & Software, Inc., a major election systems manufacturer, recently disclosed that it was working with Congressional staff on legislation to specify

---

[30] U.S. Election Assistance Commission, "Press Release: Eac Commissioners Unanimously Vote To Publish Vvsg 2.0 Principles And Guidelines For Public Comment," (Feb. 15, 2019) https://www.eac.gov/news/2019/02/15/eac-commissioners-unanimously-vote-to-publish-vvsg-20-principles-and-guidelines-for-public-comment/.

[31] U.S. Election Assistance Commission, "Fiscal Year 2010 Congressional Budget Request," (May 7, 2009) https://www.eac.gov/assets/1/6/155.PDF.

[32] U.S. Election Assistance Commission, "Fiscal Year 2019 Congressional Budget Justification," (Feb. 12, 2018) https://www.eac.gov/assets/1/6/FY_2019_CBJ_Feb_12_2018_FINAL.pdf.

[33] Robert S. Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," United States Department of Justice (2018), https://www.justice.gov/storage/report.pdf; Matt Vasilogambros, "Mueller Findings Raise Election Hacking Fears in States," Pew Stateline (May 2, 2019), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2019/05/02/mueller-findings-raise-election-hacking-fears-in-states.

an industry-wide coordinated vulnerability disclosure program.[34] This is welcome and encouraging news, as standard vulnerability handling and reporting programs can help coordinate effective response to serious vulnerability discoveries.[35] These programs should also facilitate quicker response times after published third-party independent security analyses. These types of mechanisms are especially important with cutting-edge election systems that handle actual voted ballot data – such as blockchain-mediated remote vote-casting systems.[36]

We've also seen serious problems with electronic pollbooks – often in the form of tablet or laptop computers that serve to replace paper pollbooks used to check-in voters at the polling place. Electronic pollbooks can serve as chokepoints or single-points-of-failure in polling place processes – e.g., in 2018 where voting had to be stopped for four hours in one case[37] and in another case where lines were five hours long.[38] Electronic pollbooks have not in the past been considered formal parts of certified voting systems, but this clearly must change and Congress should consider whether to simply add them to the overarching definition of "voting system" or whether a separate, more modular type of election support-system certification could suffice to better vet these systems before wide use.

Attackers will not wait until Election Day to break-in and compromise or disrupt election systems. Government systems at all levels are particularly vulnerable to attack due to the likelihood they are composed of older hardware running outdated software. Attackers scan and infiltrate government information systems, often with months elapsing before their presence is detected. Adversaries intent on disrupting March 2020 primary elections are likely sending spear-phishing emails to election officials and infiltrating election systems this very moment.

5. High Hopes For Innovative Alternatives

As we consider the future of voting, the reality is that high barriers to entry stand in the way of new entrants into the voting technology market due to the requirements for federal and state certification and testing, the wide variety of requirements for elections around the country, and the halting availability and scant nature of election funding. CDT holds high hopes for emerging market-alternative solutions such as the LA County Voting Systems for All People (VSAP) system and new models for providing more modular technologies that build off of lessons learned in much more resourced sectors to provide high levels of confidentiality, integrity, and availability. In addition, we are very encouraged

---

[34] Greg Otto, "Election tech vendors say they're securing their systems. Does anyone believe them?" *Cyberscoop* (Apr. 24, 2019), https://www.cyberscoop.com/election-security-es-s-dhs-pen-testing-idaho-national-labs-procircular/.

[35] *See:* ISO, ISO/IEC Standard 29147:2014, "Information technology – Security techniques – Vulnerability disclosure," (2014), https://www.iso.org/standard/45170.html; ISO, ISO/IEC Standard 30111:2013, "Information technology – Security techniques – Vulnerability handling processes," (2013), https://www.iso.org/standard/53231.html.

[36] Maya Kosoff, "'A Horrifically Bad Idea': Smartphone Voting Is Coming, Just In Time For The Midterms," *Vanity Fair* (Aug. 7, 2018), https://www.vanityfair.com/news/2018/08/smartphone-voting-is-coming-just-in-time-for-midterms-voatz.

[37] *Id.*, Indiana VSTOP report, fn. 17.

[38] Jessica Huseman, Isaac Arnsdorf, and Jeremy B. Merrill, "Georgia Voters Face Hourslong Waits as State Scrambles to Accommodate Turnout," *ProPublica Electionland* (Nov. 6, 2018), https://www.propublica.org/article/georgia-voters-face-hours-long-waits-as-state-scrambles-to-accommodate-turnout.

by the response of the private sector, which we hope Congress would seek to further enable, from industry leaders and start-ups.

For six years, CDT has been part of an effort lead by the Los Angeles County Registrar, Recorder, and County-Clerk, Dean Logan, called the VSAP project.[39] The VSAP system was designed from scratch to put the voter at the center of the voter experience, and to produce a highly secure, completely open, publicly owned elections system.[40] By focusing on creating a voting system that in the future any jurisdiction can own, operate, and modify, this opens the market for system integrators who may not want to invest in creating an entire voting system, but who can service, support, and deliver highly secure, usable, and affordable elections once the basic building blocks are in place.

Moving to well-managed secure cloud software products – software-as-a-service – can increase system resilience and decrease administrative burdens by concentrating expertise across many users. Similarly, commercial-off-the-shelf (COTS) cybersecurity products and services can greatly enhance the capacity of election officials and campaigns at a fraction of the cost of customized solutions. Other examples include the nonprofit election systems vendor, Voting Works[41] – a project of CDT – which focuses on producing secure and affordable voting technologies composed of COTS hardware and software. Just this week, Microsoft and Galois announced Election Guard,[42] an end-to-end auditing layer that can be easily incorporated into existing voting systems.

The private sector has also risen to the challenge, providing enterprise-class products at cost or often for free, including distributed DoS protection from Cloudflare,[43] Akamai,[44] and Jigsaw[45] and secure password management software from 1Password.[46] CDT applauds this sense of corporate civic duty to protect democracy and would like to see an increasingly broad and deep set of reduced-cost commercial cybersecurity products and services available to election officials.

6. Conclusion

I would like to once again thank the Committee, Chairperson Lofgren, and Ranking Member Davis for the opportunity to speak to you, and please do not hesitate to follow up with any outstanding questions you may have.

Thank you.

---

[39] *See:* http://vsap.lavote.net/.
[40] Kevin Monahan and Cynthia McFadden, "Has Los Angeles County just reinvented voting?" *NBC News* (May 2, 2019), https://www.nbcnews.com/politics/2020-election/has-los-angeles-county-just-reinvented-voting-n1000761.
[41] *See:* https://voting.works/.
[42] *See:* https://news.microsoft.com/on-the-issues/topic/defending-democracy-program/.
[43] *See:* https://www.cloudflare.com/athenian/.
[44] *See:* https://content.akamai.com/us-en-PG11022-elections-protection-etp.html.
[45] *See:* https://protectyourelection.withgoogle.com/intl/en/.
[46] *See:* https://1password.com/for-democracy/.

The CHAIRPERSON. Thank you very much.
Ms. Benson.

STATEMENT OF THE HONORABLE JOCELYN BENSON

Ms. BENSON. Chairperson Lofgren, Ranking Member Davis, and Members of the Committee, thank you for holding this hearing and for the invitation to testify. Securing our election infrastructure against efforts to thwart or undermine the will of our voters is essential to the survival of our democratic system. I am honored to offer my perspective as Michigan's chief election officer on this critical challenge.

As this Committee proceeds, I encourage you to seek further input from State and especially local election administrators. Now more than ever, the Federal Government's role as a partner with us securing our elections is necessary if our work at any level is to succeed. The role best manifests itself in three forms: one, investment and resources, much of which we have heard today; two, setting standards and establishing protections at the local level; and, three, setting and establishing a cooperative and bipartisan tone.

As you know, in recent years, we have seen unprecedented threats to our election system, including some from sophisticated foreign-government-aligned entities. From this very highest level of government, we need acknowledgement of the past, present, and future threats posed by foreign state actors, and through that, the marshaling of bipartisan support and cooperation to build a sustainable and secure election infrastructure in every State.

The threats to the security of our elections did not begin in 2016 and we know for certain that they will not end in 2020. Only through a unified approach and long-term commitment and investment can we adequately support the infrastructure we need to provide a voting system in which all Americans will rightly place their trust. Part of that unified approach must be a commitment to providing a predictable stream of funding and other resources.

Many of the issues we have discussed today can only be addressed partially at the local level and temporarily with the tools that we have at our disposal. In many cases, election officials know what they need to do, but they cannot afford to do it. The Federal Government has taken positive steps, such as significantly improving Federal, State, and local coordination, and making more funding available, but we need to do much more.

Michigan's election system provides a useful example. We are unique in the extent to which our election administration responsibility is shared among over 1,500 local municipalities, each one running their own elections. This decentralized system helps safeguard against systemwide problems but also means we have many links in the chain. Local officials are often on the front lines of defense, and investment in their work is critical if we are going to secure all our elections.

With that in mind, investing in the infrastructure at the local level, providing support to local clerks, supporting poll workers as well with increased accountability with local officials who don't take advantage of the resources or otherwise fail to run elections

in a way that ensures security and integrity of election results is critical.

To ensure we are implementing best practices and leaving no stone unturned in Michigan, I also formed a security task force composed of local officials, election specialists, and national experts in technology and data security, including a liaison from the Department of Homeland Security. Our goal is for Michigan's elections to be among the most secure in the country and to pilot best practices, like risk-limiting audits, that we hope can drive national reform.

While we await our Michigan panel's final recommendations later this year, their initial discussion has already focused on securing and protecting several areas of vulnerabilities. I describe these in greater detail in my written testimony but will highlight a few key points here.

First, voter registration databases. Following the 2016 election, we learned of attempts to compromise our voter registration databases in other States, some successful. If outside actors were able to manipulate registration records successfully, they could disrupt elections and put voters at risk. Protections against this potential is critical. In Michigan, we have taken steps to modernize and safeguard our voter registration database, the backbone of our election administration system. And it is also important to have protections at the local level in the event of a registration problem. Michigan has joined the growing list of States that allow voters to register on election day and vote that same day. In yesterday's elections alone, 400 voters took advantage of that freedom, and they would not have voted without it.

In Michigan, someone missing from a list on election day can now reregister at a clerk's office and vote. This is an important safeguard also to threats to challenge our voter registration databases.

In addition, voting technology is critical to upgrade, and I also want to emphasize that simple investments in voting technology is incomplete without a recognition that that technology will continually evolve, and upgrades and sustainable sources of funding for those upgrades are critical.

Finally, support from Congress and the Federal Government will be critical to ensuring this and many other issues are addressed, and I am encouraged by the bipartisan spirit of cooperation among election officials in our State and in our country, particularly when it comes to election security.

Tomorrow, Secretary Merrill, a Republican, and myself, a Democrat, are leading a bipartisan group of Secretaries of State to visit Selma, Alabama, where Congressman John Lewis and many others put their lives on the line for the right to vote. Through this leadership, we, as secretaries of state, hope to show bipartisan support and cooperation is possible, and we hope to strengthen and unify our commitment to a free and fair election system. And I encourage you to join us in this spirit of bipartisan cooperation. Thank you.

[The statement of Ms. Benson follows:]

Secretary of State Jocelyn Benson

May 8, 2019

Testimony of Jocelyn Benson, Michigan Secretary of State

Before the Committee on House Administration

United States Congress

Chairperson Lofgren, Ranking Member Davis and Members of the Committee:

Thank you for holding this hearing and for the invitation to testify. Securing our election infrastructure against efforts to thwart or undermine the will of our voters is essential to the survival of our democratic system. I am honored to offer my perspective as Michigan's chief election officer on this critical challenge. I encourage this committee to seek further input from other state officials and especially from local election administrators across the country as you proceed.

Now more than ever, the federal government's role as a partner in securing our elections is necessary if our work at any level is to succeed. That role best manifests in three forms: resources, setting standards and establishing protections, and setting a cooperative and bipartisan tone.

As you know, recent years have brought unprecedented threats to our election system, including some from highly sophisticated, foreign-government aligned entities. It is essential that from the very highest level of government there is acknowledgement of the past, present and future active threats posed by foreign state actors, and that in response we marshal bipartisan support and cooperative actions focused on building sustainable and secure infrastructure to protect our elections. Because while the threats to the security of our elections didn't begin in 2016, we know for certain they won't end in 2020. Only through a unified approach and long-term commitment and investment can we adequately support our election infrastructure and provide a voting system in which Americans will rightly place their trust.

Part of that unified approach must be a commitment to providing a predictable stream of funding and additional resources for election security. Many of the issues I will discuss today can be addressed only partially and temporarily with the tools we have at our disposal. In many parts of the country, election officials know what they need to do to improve their procedures but cannot afford to do it. The federal government has taken positive steps — such as significantly improving federal, state and local coordination and making more funding and tools available — but we need to do much more.

Michigan's election system provides some helpful grounds for examination as this committee reviews security issues nationwide. We are unique in the extent to which our election administration is shared throughout a broad range of local jurisdictions. Our elections are run

primarily by more than 1,500 city and township clerks, with 83 county clerks also carrying significant responsibilities. This decentralized system helps safeguard against state and even county-wide problems, as errors or breakdowns can be confined often to local jurisdictions. The large number of access points also means more surfaces are potentially vulnerable, however. From a statewide standpoint, with so many links in our chain, it is important to recognize that local election officials are the front line in the defense against system threats.

This also means that we need to invest in election infrastructure at the local level and provide support to local clerks. With that should come increased accountability when local officials don't take advantage of these resources or otherwise fail to run elections at a local level in a way that ensures security and integrity of election results.

I. Secure Elections in Michigan In 2020 and Beyond

To ensure we are implementing best practices and leaving no stone unturned, in Michigan I formed an election security advisory task force composed of local officials, election specialists and national experts in technology and data security (including a DHS liaison). Our ultimate goal is for Michigan's elections to be among the most secure in the country, and to pilot best practices that we hope can drive national reform. While we await the panel's final recommendations later this year, their initial meetings have focused on securing and protecting three areas of vulnerabilities: (1) our voter registration and data, (2) the process of voting and (3) the transmission of election results.

Voter Registration Databases

Following the 2016 election, the FBI and DHS determined that hackers affiliated with foreign states attempted to infiltrate multiple states' voter registration databases in that election, in some cases successfully. If outside actors were able to access a voter registration database, they could potentially manipulate voter registration records, which could wreak havoc on our election planning and possibly put voters at risk of disenfranchisement.

In Michigan, our statewide voter registration database, the Qualified Voter File (QVF), serves as the backbone of our election administration system. It is used by state, county and local election officials to run their elections and communicate with voters. In recent years, we have modernized our QVF system to improve its functionality and security.

From the voter side, we also have an important new protection against registration-based threats. Under Proposal 18-3, passed by Michigan voters last election, our state constitution now guarantees eligible Michiganders the right to register up to and on Election Day, a process that mitigates the effect of registration-based attacks should they occur. Michigan has joined a list of states offering same-day registration that has grown significantly in recent years; 17 states plus the District of Columbia now offer it in some form. Under federal law, states also must provide

the ability for voters missing from registration lists to cast provisional ballots at the polls. This is an additional failsafe, though it isn't always effective in allowing voters to cast ballots that count.

Nevertheless, a disruption to registration records has the potential to cause significant confusion and problems on and before Election Day, and protecting against this is one of the most important aspects of our work. We plan to explore and implement additional security features in addition to those we already have put in place to protect against potential attacks. Because municipal, county and state officials all access the voter registration list across our state, the cost of maintaining best practices on an ongoing basis could be significant, and federal resources have been and will continue to be critical.

Voting Technology

Michigan upgraded its voting technology in 2017 and 2018. Our localities all use one of three types of voting machine vendor systems, selected at the local level, but all are versions of optical scan machines, which use paper ballots that are scanned through electronic tabulators (with the paper ballot retained and stored). There is no evidence that voting machines in Michigan have been compromised or that votes have been changed, but in the event that a bad actor were able to alter an electronic tabulator program, using and retaining paper ballots (which can be reviewed and recounted) is an important safeguard. It is encouraging that a significant majority of voters nationwide cast votes on paper ballots, and the number could approach 100 percent by 2020.

While our voting machines are relatively new and function well, we need to ensure they remain secure and effective with continued use over multiple elections and through the lifecycle of each machine. With the pace of technology, ensuring we have adequate voting technology is an ongoing process, rather than a one-time task to be completed. Voting technology quickly and unexpectedly can become obsolete as circumstances change, and it isn't possible to ensure that all jurisdictions have the most-recent and state-of-the-art equipment with the limited funding we have available. We need to stay ahead of this curve and continue the focus on security and potential vulnerabilities of these systems.

Audits

Paper ballots can assist with another key element of election security infrastructure: auditing of election results. In Michigan, reviewing the accuracy of vote counts is mandated in our state constitution: Proposal 18-3 grants voters a constitutional right to have their election results audited. Last year, we undertook a pilot project to implement risk-limiting audits in three large cities: Rochester Hills, Lansing and Kalamazoo. Risk-limiting audits are a useful tool for verifying the accuracy of election results across an entire election (as opposed to a single precinct), because they allow us to use statistically proven methods to sample and scale the number of ballots we count and confirm election results overall, which in turn will tell us the probability that errors, manipulation or problems have occurred with vote tabulation. This is a particularly helpful feature in a state like Michigan, with our decentralized structure and where voting equipment varies across counties.

We are expanding our auditing procedures this year, with several more jurisdictions conducting risk-limiting audits in 2019. The first of these elections actually was held yesterday — May 7, when local elections were held in 65 of our 83 counties. We have a long way to go, however, to achieve a statewide audit process, which we would like to put in place as early as 2020 if possible. We hope to learn from the experiences of our own tests and those in other states.

Election Night Reporting

To bolster public confidence in election results and reduce the potential for dispute or confusion, we must ensure that electronically transmitted results on Election Night are sent quickly and securely, and that the final review and canvass of ballots is clear, transparent and error-free. And while final, certified election results cannot be delivered on Election Night, we also are examining how we can ensure as accurate an initial count as possible, as fast as possible. Discrepancies between the initial unofficial vote totals (delivered on Election Night) and the final results (certified after a thorough review and canvass in the days after the election) don't mean the actual conduct of the election was compromised. Still, we must acknowledge the reality that the initial Election Night vote total is widely shared and treated as the final election outcome by many voters, as well as the media.

We experienced the importance of this firsthand in Michigan in 2016, when our state had among the closest margins in the Presidential Election; we will see similarly close margins in 2020, if not in Michigan then surely in other states. Increased attention in a politically charged, high-stakes election magnifies the impact of any actual or perceived errors and the attendant risk of loss of public confidence in election results.

The inherent challenge in Election Night reporting is that the responsibility falls primarily on overworked, under-resourced election workers operating in a high-pressure situation at a time when they are unlikely to be well-rested. Although the polls close at 8 p.m., voters in line must be allowed to cast ballots, which means in some places voting will continue until significantly later. Once that is finished, poll workers and election officials then must close down the poll sites, ensure their unofficial results account for every ballot and every voter, and transmit their unofficial precinct results.

Increased resources for hiring and training election workers would significantly improve these circumstances. As they stand, they leave little margin for error if information sharing isn't usable and efficient for election workers; thus, improving Election Night reporting is an important area for study and improvement.

Emergency Preparedness

This decade we have seen the extent to which unexpected emergencies, such as weather events, can interfere with election processes in coastal states. Although Michigan doesn't face the specific risk of hurricanes, severe weather, power outages or worse could potentially disrupt our elections, as well. We already have important redundancies in our system, such as the ability to

conduct elections by paper during periods in which tabulators, electronic poll books and other electronic equipment are down. Nonetheless, emergency planning around election dates, particularly during high-turnout races, is a critical area of assessment that must be in place at every level in our system.

Public Communication

As important as it is to secure our elections, ensuring voters also have confidence in that security is similarly paramount. To that end, public information-distribution must be considered as an essential element of election security and integrity. Sharing accurate information broadly and quickly is particularly needed in two scenarios: to counteract misinformation, and to maintain public confidence and participation in the face of crises or unexpected events.

Misinformation poses a significant risk to election integrity in the face of organized, targeted efforts to confuse or mislead members of the public. For example, bad actors have the capacity to use social media or other communication tools to confuse the public about where or when they should vote or spread false reporting about events (for example, a fake violent or dangerous incident) that may dissuade voters from participating.

Voters also may be confused or dissuaded by unexpected events on Election Day. For example, a voter may hear a *correct* report that a polling place is experiencing problems with a voting machine and draw the *incorrect* inference that he or she won't be able to vote and shouldn't bother showing up.

In any situation in which voters are hearing false statements about the election, whether as part of an intentional misinformation campaign or through the rumor mill, election officials must be positioned to provide correct, accurate information in real-time and across all media. This requires cooperation and advance planning between state and local public officials and non-government entities, and we will be exploring how to improve our own process.

II. The Role of the Federal Government in Securing our Elections

Support from Congress and the federal government will go a long way in supporting Michigan and other states' efforts to secure our election systems. This support comes in three forms: resources, standards and protections, and setting a cooperative and bipartisan tone.

Resources and Investment: Sustainable and Reliable

Federal resources are essential tools for election infrastructure in the modern election era, starting with the passage of the Help America Vote Act of 2002 (HAVA). Most states purchased new voting machines and established statewide voter registration databases using funding made available through HAVA in the years following the law's enactment. As those resources ran out, however, election technology began to age at the same time as technology was advancing at a rapid pace.

As I discussed earlier in my testimony, Michigan recently upgraded voting machines across the state. We were able to so because we still had HAVA funds available from prior years; only with those resources was our state able to make necessary improvements in voting technology. In Michigan and elsewhere, however, we need additional support to make necessary improvements at the state and local level.

The additional HAVA funding made available last year is an important first step. In Michigan, the more than $10 million we have received will help fund the election security procedures we adopt after reviewing the recommendations of our advisory task force. We have opportunities to make further investments in registration and voting technology and boost local infrastructure using the funding we have available, but we will surely be limited in providing all the support we could to our local jurisdictions.

Federal Standards and Protections

The federal government also has a role to play in providing national standards for election security. New election security resources made available by the Department of Homeland Security have been helpful in this regard. The cybersecurity tools DHS has been able to offer are promising, and the agency has helped improve cooperation between federal and state partners through outreach and through the work of the Government Coordinating Council.

The federal government should go further, however, in identifying threats to election security and administration, providing protections against them, and promoting state and local adoption of these protections. In the past, the Election Assistance Commission has bolstered election administration across the country by certifying voting equipment and serving as a clearinghouse for information about election technology; Congress should support the agency and push it to provide more of these resources.

Setting a Tone of Bipartisan Cooperation

Election security isn't and shouldn't be a partisan issue. Federal government agencies must be mindful of their responsibility to ensure that election security doesn't become politicized. Congress should make every effort to continue the bipartisan cooperation that led to last year's additional HAVA funding, so that it is positioned to further assist the states in their election security needs in the short and long term. Although we all aspire to bipartisanship when it comes to strengthening our democratic institutions, election security is an area where we cannot afford to be divided. Without a functioning voting system, which the American people trust to deliver accurate results, we cannot maintain a representative democracy.

Despite the politically charged environment, I am encouraged by the bipartisanship and spirit of cooperation that exists among election officials in our state and across the country, particularly when it comes to election security. Tomorrow, Alabama Secretary of State John Merrill, a Republican, and I, a Democrat, are organizing a bipartisan group of secretaries of state to visit Selma, where Dr. Martin Luther King Jr., Congressman John Lewis and many others put their

lives on the line for the right to vote. My hope is that we can strengthen and unify our commitment to a free and fair election system without improper interference from outside actors.

Cooperation across partisan and state lines is possible and is essential to keeping that commitment, especially when it comes to the integrity of our voting system. I and my colleagues will continue to lead on the state level, but we hope that you and your colleagues will join us in this regard.

Thank you again for the opportunity to testify today. I hope in sharing information about Michigan's election infrastructure and the issues we are examining, I can help this committee build a strong record as it examines election security, and I look forward to learning from its review. I am happy to answer any questions you may have.

The CHAIRPERSON. Thank you very much. Good for you.
And Secretary of State Merrill.

STATEMENT OF THE HONORABLE JOHN MERRILL

Mr. MERRILL. Thank you, Madam Chairperson, Ranking Member Davis, distinguished Members of the Committee, I am honored to be with you today. I am John Merrill and I have the privilege to serve as Alabama's 53rd Secretary of State. Alabamians have an extraordinary amount of experience with effective and ineffective election administration. At one time, our laws were written to reduce or eliminate minority participation in the electoral process. My team and I work diligently each day to ensure the right to vote and the opportunity to receive a free government-photo-issued ID are extended to each and every eligible U.S. citizen that is a resident of our State.

Since I have been Secretary of State of Alabama, we have broken every record in the history of the State for both voter registration and voter participation. I will get to those numbers in a few minutes, but I think that it is essential to impress upon the Committee and members of the body and my fellow citizens of the United States that we cannot solve one crisis by pretending it is another. We must work collectively to strengthen our cybersecurity to protect the integrity of the electoral system from foreign influence. However, we should not present a narrative to citizens that only one system can ensure an equal right to vote.

As I previously stated, my goal as Alabama Secretary of State is to ensure that each and every eligible U.S. citizen that is a resident of our State is registered to vote and has a photo ID. During my time as Alabama Secretary of State, my team and I have changed the paradigm for voting in the State of Alabama. Since January 19, 2015, we worked with notable Alabamians, local officials, interested parties, key communicators, and concerned citizens to encourage voter registration and voter participation. The results are staggering.

Since January 19, 2015, we have registered 1,249,422 new voters. We now have a record 3,479,068 registered voters. I am very, very proud of that because we have led the Nation per capita in those numbers since I have been the Secretary.

You also need to know that we have got 30 of our 67 counties that have electronic pollbooks which expedites the check-in process and offers greater security for voters to participate in the process. As a part of our efforts to ensure voter integrity, we have worked to secure six convictions on voter fraud, and we have had two elections that have been overturned.

We will continue to document, investigate, and prosecute those individuals and their attempts on disrupting the electoral process for others.

We have created Alabama's first Braille voter guide and other applications for absentee ballots printed and regular ballots printed in Braille. In 2016, we created a committee to author and pass legislation and make it easier for folks to regain the right to vote after being convicted of disqualifying felonies.

My legislative team is currently working with Alabama State Senator Rodger Smitherman, a Democrat, to pass legislation, to

make it easier for Alabamians to cast an absentee ballot, including those Alabamians that are incarcerated but not convicted of disqualifying felonies while they remain incarcerated.

Our director of relations is currently working with a team of election analysts and other third-party groups to build an active pilot program for the most effective manner which we can conduct post-election audits. We have worked to secure election systems that do not connect to our State and local internet networks for potential breaches of internet connectivity.

We have expanded training provided by the Office of the Secretary of State to make sure that cybersecurity is included.

All these efforts are designed to ensure that we have made sure that we are providing the safest and securest election procedures in our State. We have broken every record in the history of the State for voter participation in the last four major elections that we have had as well.

We also have an electronic, election-night-reporting system, which has been exceptional and has been a model that other States have used. As a matter of fact, when we had our special U.S. Senate election on December 12, 2017, we accommodated more than 500,000 unique voters and users who were monitoring the system at one time. The work that we completed in advance of the election with our State and Federal partners to ensure that the system was secure and could be able to withstand cybersecurity attacks has been notable and has been successful. All we are trying to do is to make it easy to vote and hard to cheat. There is a number of ways that we have continued to do that.

I think the most important thing for me to close with is by sharing that we continue to work with our private and public partners, and the effort that Secretary Benson and I have put together to ensure that we are trying to do the best we can to have a bipartisan effort to help people understand where we are today in our elections process and where we hope to be in the future. We think the best way to do that is by understanding each other, each other's needs, what our common goals are, and how we hope to move forward for the future. Thank you so much.

[The statement of Mr. Merrill follows:]

Statement from the Honorable John H. Merrill
Alabama Secretary of State

Before the Committee on House Administration

U.S. House of Representatives

May 8, 2019
Washington, D.C.

Chairperson Lofgren, Ranking Member Davis, and Members of the Committee, thank you for the opportunity to come before you today to discuss election administration and cybersecurity.

My name is John Merrill, and I am Alabama's 53rd Secretary of State.

Alabamians have an extraordinary amount of experience with effective and ineffective election administration. At one time, our laws were written to reduce or eliminate minority participation in the electoral process. My team and I work diligently each and every day to ensure that the right to vote and the opportunity to receive a free, government-issued photo ID are extended to each and every eligible Alabamian that is a resident of our state.

Since I have been the Secretary of State, we have broken every record in the history of the state for voter registration and voter participation, and I will get to those numbers in a moment, but I think that it is essential to impress upon this committee, members of the body, and my fellow citizens of the United States, that we cannot solve one crisis by pretending it is another. We must work collectively to strengthen our Cyber Security to protect the integrity of the electoral system from foreign influence; however, we should not present a narrative to citizens that only one system can ensure an equal right to vote.

As I have previously stated, my goal as Alabama's 53rd Secretary of State is to ensure that each and every eligible U.S. Citizen that is a resident of Alabama is registered to vote and receives a photo ID.

During my time as Alabama's Secretary of State, my team and I have changed the paradigm for voting in the State of Alabama. Since, January 19, 2015, we have worked with notable Alabamians, local officials, interested agencies, key communicators, and concerned citizens to encourage voter registration and voter participation. The results are that we have registered 1,249,442 new voters, which brings our total number of registered voters to 3,479,068. Thirty of our 67 counties use electronic poll books, which expedites the check-in process and offers greater security for the voter and greater efficiencies and accountability for the poll worker. Our stated goal is to have electronic poll books in every county in the state by 2022. As a part of our efforts to ensure voter integrity, we have worked to secure six convictions of criminal activity related to voter fraud and will continue to document, investigate, and prosecute those individuals' intent on disrupting our democratic institutions for personal or political gain.

We have created Alabama's first braille Alabama Voter's Guide and offer applications for absentee ballot printed in braille. In 2016, we created a committee to author and pass legislation to make it easier to regain the right to vote after being convicted of a disqualifying felony, and my legislative team is working with Alabama State Senator Rodger Smitherman, a democrat, to pass legislation to make it easier for Alabamians to cast an absentee ballot. Including those Alabamians who are incarcerated but not convicted of a disqualifying felony conviction, while they are incarcerated.

Our Director of Elections is working with a team of election analysts and other third-party groups to build an active pilot program to test the most effective manner in which our state should conduct post-election audits. We have worked to secure election systems that connect to

our state and local networks for some form of internet connectivity. We have expanded the training provided by the Secretary of State's Office to local election officials to include cybersecurity and how to handle the increased cyber threat in the world today.

All these efforts have helped our citizens become more involved and engaged in the process to elect officials that represent them in local, state, and federal positions. We have broken every record in the history of the state for voter participation, as Alabamians have turned out to vote in record numbers. In March of 2016, we set a record for voter participation in a presidential preference primary with 1.25 million Alabamians casting a ballot. In the General Election on November 8, 2016, 2.1 million Alabamians cast a ballot. Alabama then broke the record for participation in a Special Election during the 2017 U.S. Senate Special Election, held on December 12, 2017, with 1.3 million Alabamians casting a ballot for their choice for the next U.S. Senator from Alabama. Most recently, we broke the record for turnout in a non-presidential general election year during the 2018 General Election with more than 1.7 million Alabamians going to the polls.

We have also worked with the Chief Election Official at the county level in Alabama, the Probate Judge, to ensure that unofficial Election Night Results are securely transmitted through encrypted channels to the Secretary of State's Office. Our team verifies the data submitted and then makes that available in real time to the public and members of the media. This system was built to withstand technical challenges, and during the 2017 Senate Special Election, our site was able to support more than 500,000 unique users at one time. The work we completed in advance of the election with our state and federal partners to ensure that the system was secure and could withstand DDoS and other similar cyber-attacks allowed Alabama to be prepared for both the threat from actors who wish to cause harm and the flood of users with an interest in the result of the election.

In Alabama, we are making it easy to vote and hard to cheat.

As we prepared for the 2018 General Election, we worked to ensure our systems were protected by requiring 2-Factor Authentication for any state or local user who accesses the voter registration system. We secured our networks and our election night reporting system with resources provided through the Department of Homeland Security, our local information systems team, and other third-party vendors. Our work to conduct elections efficiently and effectively is supported both by the Elections Assistance Commission and the Department of Homeland Security. The EAC provides guidance and support, as we prepare our local election officials to administer their elections. Our relationship with DHS is a relatively new one, but it is one that has been home to significant growth over the last two years. Prior to the Senate Special Election in December of 2017, we had very little interaction with DHS. However, as that election approached, we were able to work closely with DHS to ensure our systems were secure. We wanted to make sure that any vulnerabilities that we could identify were resolved and any new issues were mitigated before they disrupted an election in Alabama. We have also hosted a team from DHS onsite with us throughout Election Day to ensure issues are resolved in real time.

In closing, I think that it is imperative that the federal government learn from the bi-partisan nature of the National Association of Secretaries of State (NASS). At the Annual Winter 2019

Meeting of NASS members, I was approached by Michigan Secretary of State Jocelyn Benson, a Democrat, who presented the idea of hosting the Secretaries in Alabama for a tour of the historic sites located in our state, which tell the story of how Alabama and its citizens found themselves on the forefront of the fight for civil rights. That is why tomorrow begins a three-day tour, which begins in Birmingham, Alabama at the site of the 16th Street Baptist Church that was bombed September 15, 1963 during the peak of the Civil Rights Movement. We will then spend a day in Montgomery and a day in Selma visiting historic sites and studying the sacrifices made to ensure that all Americans are able to enjoy the right to vote.

As the state's chief election officials, we have an extraordinary amount of responsibility to ensure the integrity of the electoral process is secure and preserved. We have also seen that the most effective way to combat foreign influence in our elections systems is to work with our colleagues across the country to share information and to work together to ensure that our people can remain comfortable casting a ballot and confident in the results of the election.

The CHAIRPERSON. Thank you very much.

And thanks to all the witnesses.

Now is the time when Members of the Committee may ask questions of the witnesses for five minutes apiece.

I will turn first to our Ranking Member, Mr. Davis, for questions that he may have.

Mr. DAVIS of Illinois. Well, thank you again to all the witnesses for your testimony.

I want to start with Mr. Hall. Assuming the supply chain is secure, do you believe that ballot-marking devices with a voter-verified receipt is a reasonably secure method of voting?

Mr. HALL. Absolutely. One of the things we struggle with here is to make a system a hundred percent secure is impossible.

Mr. DAVIS of Illinois. Okay.

Mr. HALL. What we try to do is make them as secure as we can. Certain ballot-marking devices, they are not all created equal. I have my favorite, which is created by a government, the county of L.A., Los Angeles County. But I do think that, especially if we can make sure that voters understand that it is their civic duty to make sure they look at that piece of paper that is the ballot of record, that it is a secure and reasonable system.

Mr. DAVIS of Illinois. Okay. What, in your opinion, would the sample size be for a risk-limiting audit in a State like Florida with a 10,000-vote margin in a statewide race?

Mr. HALL. The example I typically use—I don't know the details about Florida, but for example, in a State like California, a 1-percent-margin race, typically to get around 95 percent confidence, you need to sample 400 ballots from the entire State. So this is why risk-limiting audits are so awesome because they give you the best leverage off of counting the fewest ballots to know, if you did a recount, it wouldn't change.

Mr. DAVIS of Illinois. But do you think the risk-limiting audits would result in more statewide recounts?

Mr. HALL. I like to think of these as statistical recounts. You get the answer you would get from a recount without having to do the recount. I am hoping—I doubt that would be the case, if you were going to go to a recount before, that you would probably go to a recount under these systems as well.

Mr. DAVIS of Illinois. Okay. It wouldn't work in my 2,000-vote margin of victory, huh?

Mr. HALL. It depends on a number of factors. It is hard for me to say without doing the math——

Mr. DAVIS of Illinois. Sample size of, like, two.

Mr. HALL. Yeah. Probably not.

Mr. DAVIS of Illinois. Hopefully I can get my wife and kids. So, could State-canvas systems already in place be modified for risk-limiting audits?

Mr. HALL. This depends on a bunch of technical factors. The best risk-limiting audits right now are what we call ballot-comparison risk-limiting audits, where a single ballot is compared with the digital record that it corresponds with. Those are only feasible right now with what are called central count optical scan systems, and so it depends on the specifics of the locality——

Mr. DAVIS of Illinois. Okay.

Mr. HALL [continuing]. Whether or not they are—we are working on making it work for everything, but it is going to take a little while.

Mr. DAVIS of Illinois. Well, that gets me to my next question. How does the Center for Democracy and Technology through its support of Voting Works hope to impact the current market for voting systems and election support?

Mr. HALL. Voting Works is—nonprofits will incubate other nonprofits when they don't have their 501(c)(3) status, and that is what we are doing at the Center for Democracy and Technology. Voting Works aims to be a nonprofit, open-source, voting-system vendor, which is very different than all the other election manufacturers on the market. We hope that by building things that people can take and use and build on, that through that work, it will spread good things rather than keeping things proprietary and keeping things secret.

Mr. DAVIS of Illinois. Okay. Mr. Norden, do you believe that an equal protection claim under the Voting Rights Act would exist in relation to post-election audits?

Mr. NORDEN. I am not sure I understand the question. Are you saying that if a jurisdiction didn't conduct post-election audits, would there be an equal protection claim?

Mr. DAVIS of Illinois. What I am saying is, if they did a risk-limiting audit and a jurisdiction made the claim, would you believe that if it was compared to another neighboring jurisdiction, that the—that the equal protection claim under the VRA would exist in relation to the post-election audits?

Mr. NORDEN. I guess what I would say, this is the first time I have ever confronted that question, so I would have to think about it, but it would not immediately occur to me that somebody could bring an equal protection claim for how post-election audits were conducted.

Mr. DAVIS of Illinois. Okay. Yeah, I would like you to think about it and get back to me——

Mr. NORDEN. I am happy to do that.

Mr. DAVIS of Illinois [continuing]. If you could.

Okay. And then to the entire panel and whomever wants to answer, what, if anything, do you know about the U.S. Department of Defense Advanced Research Project Agency's effort to create a federally supported hardware architecture for voting? And do you believe the Federal Government should be pursuing a more aggressive role in the design and deployment of elections technology for State and local adoption, and if so, why or why not?

Mr. MERRILL. My answer is no, and the reason is because that should be left up to the local States to be able to purchase the equipment that they think is important for them to use. And, frankly, I feel like the free market is the one that ought to determine what the availability of that equipment is and what should be purchased and what should not as long as it meets the standards.

Mr. DAVIS of Illinois. Okay.

Ms. Benson.

Ms. BENSON. I would actually—I would welcome that type of investment at the Federal level. The work that we have done already

with the Department of Homeland Security has been very helpful because of the additional resources and expertise they bring to the table. I do think it would need to be a partnership with States and local election officials who have unique things to share as to what the infrastructure should look like, but certainly I could only imagine that it would help our efforts to secure our elections if we had that level of infrastructure, investment, and support.

Mr. MERRILL. And to be clear, we are still friends.

Mr. DAVIS of Illinois. So are we.

Mr. MERRILL. But I am not for universal adoption.

Mr. HALL. So, quickly, the work that DARPA is doing is to create secure hardware and to use voting as a really challenging application on top of that. And the cool thing about that is it will be usable by anyone later down the line who could actually take that and turn it into a product, rather than a research demonstration system, so I am very hopeful that this will benefit everyone in a way that doesn't force them but allows them to see that secure hardware is a really important part of securing systems in general.

Mr. DAVIS of Illinois. Thank you.

The CHAIRPERSON. Thank you. I will recognize myself for five minutes because I want to follow up on this DARPA issue. I had understood, perhaps incorrectly, that they were also—DARPA was also looking at open-source software. Is that correct, Mr. Hall?

Mr. HALL. As far as I understand it—and I am not involved in the project—there is a hardware component. There is the software that runs on the chip that they are making, and then there is the software around the application of voting itself. So there are a bunch of pieces in there. I am pretty sure that all those pieces are going to be freely and publicly available under generous copyright licensing terms. And I think that is——

The CHAIRPERSON. Does anyone else, any of the other witnesses—we have reached out to DARPA, and they thought it was best not to be a witness at this hearing. But do you know, Mr. Norden? No? So I think we need to know more about that because it seems to me that we have had a problem in the country with proprietary software systems refusing to tell anybody what their system is not disclosing, and so the victims ultimately are the American voter, but also election officials can't know what the problems are even if they should be concerned about what had happened, and having open-source material available to elections officials is one way to avoid that.

I would like to follow—or perhaps you don't know, Mr. Hall, but some of the software experts in my home, Silicon Valley, were critical about the DARPA effort, that it wasn't sufficiently open source to their liking. Do you know anything about that?

Mr. HALL. I am not familiar with it. I would have to follow up.

The CHAIRPERSON. I think we need to pursue it with DARPA then.

Let me ask you this, Mr. Hall, or anyone else, Mr. Norden, how should political campaigns, which are fast-paced, nimble, in a rush, bolster their cybersecurity, particularly if resources are scarce? Usually, oftentimes, it is the last thing the candidates are thinking about. What are best practices for campaigns?

Mr. HALL. Many of the best practices for campaigns are very similar to the best practices for election officials, or you can even think of a campaign as really a rock 'n' roll startup. They only last for, like, 18 months, and it has a ton of money and has to get rid of it really quickly. The things that can really help the campaigns are what I call of systems-level protection. So, for example, hardware keys for two-factor authentication, where it is not just a password that you have, but you actually have to have something on your key chain that you stick in and push a button. Those things, and then hardening their communications infrastructure. So there have been a lot of attacks on email systems of campaigns and things like that. These are things that we can deal with. The problem is a campaign's security is not the thing that they get awards for doing well, right? They get someone elected. And so——

The CHAIRPERSON. Right.

Mr. HALL [continuing]. A lot of us have been trying to change the mentality and say: Look, security is just as much a first-class citizen in your enterprise as it is——

The CHAIRPERSON. Well, especially if it has an impact on whether you get elected, so——

Mr. HALL. Absolutely.

The CHAIRPERSON. Mr. Norden, you have written books and articles on this subject. Describe, if you can, what hacking into election systems, whether it is voter registration databases, the voting machines themselves, what could happen on election day? What is the worst case—what keeps you awake at night on this?

Mr. NORDEN. Oh, gosh. Look, you know, in many ways, we know—we know some of the bad things that can happen by looking at what has happened in other nations, but we also know just what has happened not by malicious act but by mistake here in the United States. And I often say that anything that can happen through error is kind of the opposite side of the coin of what can happen maliciously. We have seen, for instance, when electronic pollbooks fell, what kind of chaos that can cause at the polls, how it can keep people from voting, how it can cause lines for hours. And so that is certainly something that I worry about, and I am concerned that we don't have Federal standards, unlike for voting machines. I think when HAVA was written, electronic pollbooks weren't in as wide use as they are today. Thirty-four States use them today. And we don't have those kind of baseline—you know, the voting machine guidelines are voluntary. If we had something like that at the Federal level, I think that could be a baseline for States. We have information—a lot of these electronic pollbooks use wireless components. They have information that is on the cloud. So that is something that worries me, of course. And same thing with—and that is an example of the kind of thing that you would be worried about with registration databases also, changing information so that when people show up at the polls, they are unable to vote. There is a lot that we should be doing, and I think we can be doing, to protect against that, making sure that we have contingency plans.

And then, lastly, of course, the real—the nightmare—the big nightmare scenario is that somehow somebody changes votes on a voting machine or for election night reporting, and I do think that

is why having paper backups of every vote, being able to go back and, detect it through audits, and then recover. And I think that is important even if there isn't an attack. They are so—you know, when we talk about foreign interference, we are often focused on election infrastructure. There is a whole social media disinformation element to this that Mr. Davis mentioned. There can be a lot that is done there to undermine confidence in the vote, and having paper backups, doing audits, I think, is one way to combat that.

The CHAIRPERSON. Thank you very much. Before calling on the gentleman from Georgia, I will say, we had very strongly held divergent views on various elements of H.R. 1, but I don't think there was any disagreement on a partisan basis that we want every vote cast by Americans to be counted as cast, and that we don't want to become victims of an attack from any source. I think there is bipartisan agreement on that.

The gentleman from Georgia is recognized.

Mr. LOUDERMILK. Thank you, Madam Chairperson.

It is a very important hearing we have here, and I have got a couple questions, especially regarding the voting machines. I come from a technology background. I have an IT background. Also, early in my career, I had a job spying on Russia, in the Air Force. I bring a cybersecurity aspect to this as well. Long-time advocate for a paper backup. But what I am hearing, it seems counterproductive to some things I have advocated for in the past because I have seen the advantage of computer-based voting is the efficiency, especially when it comes to post-election. I can remember the first elections I was involved in, as a volunteer. You were up till midnight, 1 or 2 o'clock in the morning, in Georgia, waiting for results to come in. People are sitting at the courthouse waiting for counts to be done. We brought electronic voting in. A lot of times you know within a half hour to an hour by the time the polls close.

But then we have the problem of, I would get calls from Republicans that the machines were changing my vote as I voted to all Democrats, and you get the same thing from the other side.

What I heard from a lot of you is to not use a paper backup but use a predominantly paper ballot system with a computerized backup, which seems to be backwards to me from what would be the most efficient use, which would be, utilize computerized voting because of the efficiency. We already have a lot of long lines and the initial counting, but have the machine produce a paper verification that the voter then verifies that piece of paper is what they cast on the machine, that is then filed and used as a backup. I would like to hear, Mr. Hall, what are your thoughts on that? Because to me that actually reduces the human error, multiple marks made on a page for the same candidate, hanging chads, all that, is that the voter is then verifying that the computer did take what they said—the way they voted, and then that would be used for your recount.

Mr. HALL. Yes, and so what I would say is, we have come a long way since around 2000 in that the machines we use now and that we are advocating for are what we call software independent. And what I mean by that is that no change in the vote total is—I am misstating the definition, but essentially think of it as, if something

were to mess with the vote totals, you would still have an independent way of coming at the actual result. And so now these ballot-marking devices, they don't keep any state, to use a nerd word. Now, they don't keep the totals themselves. They use a different machine, like an optical scan machine, to suck the ballot in and actually do the counting. And so you have the benefit of using technology——

Mr. LOUDERMILK. Right.

Mr. HALL [continuing]. For doing all of the navigation. You have a computer counting the thing, and you still have a paper ballot backup for the auditing.

Mr. LOUDERMILK. So you have an IT-based device that actually casts the paper ballot, and a different device that actually counts it, and you have a backup.

Mr. HALL. It depends on the model, but yes, that is basically correct.

Mr. LOUDERMILK. Okay. Ms. Schneider.

Ms. SCHNEIDER. So, the way you described the paper ballot working is actually the way that it does work with an optical scanner. You are still getting the efficiency of the computer when it comes to ballots, and you can still have that speed, although we should consider whether speed is the value we want on election night, but you still have that speed by having the computer scanners, even if you mark a ballot by a pen or pencil.

And I do want to point out that with ballot marking devices, it is critically important, especially if they are used for all voters, there are two critical important things: One, there has to be enough. You have to know how many voters can vote on a single device during the course of one election day; and two, there has to be a process, a deliberate process, especially for those who are not using the assistive features to deliberately verify that their choices are correctly reflected, because there could be mistakes, or there could be malware that could impact that ballot, and so you have to—that is a process. That is a process issue on top of a security issue.

Mr. LOUDERMILK. So let me make sure. You are talking about actually using a physical ballot that I mark.

Ms. SCHNEIDER. Right.

Mr. LOUDERMILK. Like the standardized tests that we used to do in school.

Ms. SCHNEIDER. That is correct.

Mr. LOUDERMILK. Does that not open up for human error that takes us back to the hanging chad days of the 2000 Presidential election?

Ms. SCHNEIDER. We use paper ballots in my home county. I will tell you a story. In the State House race in my county, the margin of victory was about two dozen votes. It happened twice, in 2006, and, again, in 2016. And about 23,000 ballots were counted in that race. There was a full hand recount of those races, and the ambiguous ballots that you would talk about where you might dispute the voters' intent were not enough to change the outcome.

Mr. LOUDERMILK. But if we could, Mr. Hall, you seem to be agreeing with me in that aspect as it does open up the chance for

human error but doing it the way we were discussing would pretty much alleviate that. Is that true?

Mr. HALL. Yes. And I think this is where we differ a little bit on the panel in the sense that at CDT, we believe that using the computer interface to improve navigation to reduce errors is a really important part. You do need to have enough of them. You have to pay for them. They are really expensive. And, so, those kinds of balancing features come into the ultimate decision of whether or not you should purchase those kinds of machines, but we believe that you should use technology when it does things really well and then ground it, you know, have it in something like paper when there is an important security element that you can't otherwise do. It is like an "air gap."

Mr. NORDEN. I would just quickly like to add one thing. The Brennan Center doesn't take a position on ballot marking devices versus optical scan and filling out these ballots, but I do want to make one point. Most people at this point in the United States are voting on these paper ballots now, and the scanner, as a computer, can be very helpful in preventing the kind of problems that you are talking about. In fact, the new technology makes it much less likely that somebody makes a mistake that they can't catch. The scanner now will notify a voter if it can't read their vote, will notify a voter if they voted in too many contests.

So, the kind of hanging chad problem that you are talking about because of that technology is much, much, much less frequent. We have statistics on this, much, much less frequent than we saw with punch card ballots.

Mr. LOUDERMILK. I see my time expired, but maybe if we have a second round, Madam Chairperson, I will follow up.

The CHAIRPERSON. Sure. The gentlelady from California, Mrs. Davis, is recognized. And as I have to attend a meeting I cannot get out of, so I am going to ask her to take the chair.

Mrs. DAVIS of California [presiding]. Thank you. I was going to thank Madam Chair, but I want to thank all of you for being with us today. I appreciate it very much.

I want to ask you, please, Mr. Hall, if you could walk us through the process, or maybe it is even the lack of a process, on how the NSA lets State election officials know about emerging threats, or vulnerabilities that they have discovered in State election infrastructure?

And I will go on for just a second and be a little bit more specific. Is there a formal system already in place for when the NSA or the broader intel community is supposed to communicate with State election officials? From what I understand, there is something that has been created called the Vulnerabilities Equities Policies and Process, but it doesn't appear that it has the kind of proactive warning that private industry or State election officials can do anything with, or at least it doesn't seem to notify them in real time so they can respond.

Mr. MERRILL. Madam Chairperson, obviously you didn't ask that question, but not to overstep, I think it is important——

Mrs. DAVIS of California. Sir, let me ask Mr. Hall first, okay?

Mr. MERRILL. Yes, ma'am. Just to let you know, we didn't receive any notification from anybody at any time.

Mrs. DAVIS of California. Okay. No. That is part of how we deal with this, yeah.

Mr. MERRILL. Yes, ma'am.

Mr. HALL. Okay. So there were two things in your question. The first is how State and local election officials are notified of potential attacks on their systems. This is a pretty well-orchestrated thing. I don't know the full details, but I can give you a high level overview, and if you ask me in Q&A format, I can follow up in more detail.

Essentially, the NSA does, and the CIA do things, and not in the United States, to figure out who may be attacking our systems. The FBI does a little bit of that, too, domestically. If something were to happen where someone foreign was targeting our systems with cyber-attacks, presumably, the FBI would be notified, and either DHS or FBI, probably FBI, would notify the State and local election officials.

In some cases, that went to governors or CIOs who may not be in the path. They may not have been directly plugged into that disclosure path. I think that is changing now with clearances for the State officials, because often, if you don't have a clearance, you can't accept this kind of stuff. So it is cleaning up a little bit.

I still think that I am seeing, for example, there is a problem—if you are a victim, when DHS notifies you, they are not going to announce to the world what happened to you. It is up to you as the victim to disclose that, or it is going to come out in the press at some point. That thing—I think there needs to be something, like a couple of years or a year after something—someone gets notified such that that stuff becomes public.

The Vulnerabilities Equities Process is something I can describe. It is a little different in that it is more about flaws that our defenders find, or offensive people find in commercial products that they can then decide when to disclose to the commercial entity to fix them. And I haven't seen that touch the voting systems sphere yet. It would be interesting if it did. I would love to know about that.

Mrs. DAVIS of California. Yes. Thank you. Really, I respect your response there. What we are trying to figure out is, is there a way to have clearances and then the issue is, what do you do? If you think about it, say you get that information a few days before an election, and it is very serious.

Mr. HALL. That is very tough.

Mrs. DAVIS of California. What do you do?

Mr. HALL. It depends on the nature of the information. For example, if you are told that someone installed malware on one of your machines, and it hopes to spread to your other machine, because they know exactly what the machine is, hopefully, you can quarantine that machine. But often, it is more likely there has been someone in your network for six months. We have no idea of what kind of access they had. You need to look at everything. That can be a real, real challenge for local elections.

Mrs. DAVIS of California. So part of it, perhaps, may be—and if you all want to respond, just the vulnerabilities that you may learn about, but that may not necessarily translate into something that you can act on, in real time. So that is something that—I think we

all need to be thinking about that and how we can be helpful to you as election officials.

I wonder, Secretary Benson, if you were to suspect a foreign intelligence hack, who would you turn to? Where would you go from there?

Ms. BENSON. We have contacts, you know, with DHS and multiple different agencies, so we would contact, you know, whether—regardless of the potential threat, and we are in, and I am in, frequent contact with those officials. In fact, we have a DHS liaison at Masterson who serves on my election security task force, so we are in frequent communication. That is something I established early on in my tenure to ensure that we are, in real time, learning of threats, and then, you know through security clearance.

Mrs. DAVIS of California. Any ideas that you all have discussed that you think, perhaps, we need to know about in terms of how you can have a better relationship in this way?

Ms. BENSON. I think it is a proactive one on the part of the Federal Government, as well as the Secretaries of State, that perhaps standards and expectations from Congress can establish. But it is something that an individual leader will take seriously, but I think encouraging us to develop that relationship and then ongoing communication and a statewide response system is important.

Mrs. DAVIS of California. Okay. Thank you very much. I am sorry.

Mr. Butterfield. It looks like it is your turn.

Mr. BUTTERFIELD. Thank you very much. I know the Chairperson is not in the room, but I want to begin by thanking her for holding today's hearing. This topic is extremely important. It appears to be a bipartisan issue that we are talking about, and one that is very dear to my heart.

The Mueller report that we have heard so much about has a revelation that I want to make a reference. The Mueller report stated, quote, "In August of 2016, the GRU officers," and, of course, we all know that is the Russian foreign intelligence agency, "targeted employees of," and then there is a redaction, "a voting technology company that develops software used by numerous U.S. counties to manage voter rolls and installed malware on the company network."

Further, the report goes on to describe a separate spear-phishing operation conducted by GRU operatives that enabled access to the network of at least one Florida county government. And now, I am just finding out that in my Congressional district in North Carolina, a poll book product provided by an election vendor catastrophically failed on Election Day in 2016. Now, that failure occurred in six precincts in Durham, North Carolina on Election Day. And one of those precincts was forced to close one hour and a half at lunchtime during one of the busiest times for voters.

There has been reporting that the voting technology company identified in the report, that is the Mueller report, who suffered a cyber intrusion in August of 2016, is the same vendor whose poll books catastrophically failed on Election Day in my district. The intrusions described in the Mueller report demonstrate just how important today's hearing is, and how robust action is urgently need-

ed from this Congress to ensure the security and integrity of our election system.

We know Russia interfered in our elections in 2016 and will likely try it again next year. And so, the question is then presented: What is this Congress going to do about it? Let me start with you, Mr. Norden. Was the attack in 2016, in your opinion, a well-planned Russian attack, or was it basically spontaneous?

Mr. NORDEN. Thank you for the question, Mr. Butterfield. That is something I have thought a lot about. If you look at the reports of what the Russians did, actually, the attacks on election infrastructure almost look like an afterthought. They happened months after the hacking of political campaigns, at least reported what we know, months after the hacks on political campaigns, and years after the first disinformation campaign that we saw from the Russians.

I do have concerns that—this is one of the reasons why I am concerned that the threat we face in 2020 is greater. The Russians will now have had four years to gain whatever they learned and given what we know that they have done in other countries, I would be concerned that there is potentially a much more aggressive action.

Mr. BUTTERFIELD. Let me talk about election vendors for a moment, if I can. Can you quantify for me the number of election vendors throughout the country? Is it a small number?

Mr. NORDEN. Well, that is a very difficult question to answer, because election vendors are central to so many aspects of the elections we run. We often think about just voting machines, and there are three main voting machine vendors and a couple of other smaller ones, but then there are vendors that produce electronic poll books. There are vendors that, for some local election offices, create their websites.

Mr. BUTTERFIELD. Is there a registry anywhere of election vendors?

Mr. NORDEN. Not that I am aware of.

Mr. BUTTERFIELD. What regulatory oversight does the Federal Government have over an election vendor? Do we have any oversight?

Mr. NORDEN. So, I mean, at the moment there—one thing that I talk about is there are more Federal regulations of ballpoint pens than there are of our election infrastructure. There hasn't been, as far as I am concerned, as much oversight as there should be of election vendors. We don't necessarily know who owns the election vendors. We don't know who works for them.

Mr. BUTTERFIELD. Are you a proponent for more oversight?

Mr. NORDEN. Absolutely. Absolutely. I think we need more information about who the vendors are, who works for them, what kind of security processes they have in place. And I certainly think a basic thing that we deserve is if election vendors are aware of a cyber attack on them, that they should be required to report that to the Federal authorities, to anybody that is using their products, and that currently doesn't exist right now. There is no requirement for that.

Mr. BUTTERFIELD. That was going to be my next question.

Yes. Ms. Schneider.

Ms. SCHNEIDER. Thank you. I wanted to answer your other question regarding the number of vendors. The reason it is so difficult to determine that number is because there are 8,000 jurisdictions who administer elections, and for many of those jurisdictions who are very small, they outsource or contract with vendors to perform many steps in the election administration, and so, the real oversight need is for these third-party vendors. They may not be voting system manufacturers, but they may provide services and exactly the kind of vendors that you are talking about from the Mueller report where there is no oversight or regulation of those vendors, and no standard that they have to adhere to in terms of cybersecurity.

Mrs. DAVIS of California. Thank you. Thank you for your response.

Ms. Fudge.

Ms. FUDGE. Thank you very much and thank you all for being here. As you may know, we have been traveling the country a bit just getting data and information about voting irregularities, voter suppression, et cetera. I want to start with the two elected officials that are sitting here.

We have heard so much as we have traveled the country. I am from Ohio, by the way, a State that thought that our machines were so awful, we got rid of them, but South Carolina bought them. This is true. South Carolina bought all the machines we got rid of because they were not effective. To go back to your point, there is no regulation.

I am trying to determine from the two of you what do I tell people who have no confidence in our system? What do I tell people who believe that there is no integrity, that don't believe that their votes count? I have people who are afraid now to vote absentee, but then they come to the polls and see long lines, and they are afraid to do that, too. They look at these electronic books and they can't find their name, and when they do, their signatures just may have dotted their "I" differently, and they tell them they can't vote. What do I tell people who have no confidence in the system? What the state is of voting—what is the state of affairs of voting in the United States today?

Ms. BENSON. I think you tell them, one, that we have much—one, I completely agree that focusing on ensuring voters have confidence in the security and accessibility of our elections is a critical component to making our democracy work. And I think why it is so important that we have a partnership at the State level with Federal Government, and why the Federal Government can set important standards and play an important leadership role, just as it has historically with the Voting Rights Act. It is setting the standards and expectations that States must meet in order to protect everyone's right to vote.

In addition to that, I think factually, and what you have heard today, is that we are further ahead than we were five years ago, two years ago, ten years ago in securing our elections, but as we have moved forward, threats have emerged as well and evolved. And so what we need more of that we haven't had before is a stronger Federal and State partnership, and even Federal-State-local paper partnership where we are collaborating on a bipartisan

basis to ensure that we are leaving no stone unturned in promoting the accessibility of the vote and the security of the vote. Those ongoing communications, that ongoing partnership, is important, and that is part of what we have tried to do at the State level among our Secretaries.

Mr. MERRILL. Yes, ma'am. I think it is real important to note some of the things we have already introduced. First of all, in our State, we made a concerted effort to ensure that people know that their vote needs to be cast for the candidate of their choice, but in order to do that, you have to be a registered voter, so we made it a campaign effort to ensure that all eligible people in our State are registered to vote. 96 percent of all eligible African Americans in the State of Alabama are registered to vote, 91 percent of all eligible Caucasian Alabamians are registered to vote, and 94 percent of all eligible Alabamians are registered to vote.

Ms. FUDGE. But that doesn't tell them that their vote counts.

Mr. MERRILL. No. But, when they go to all 2,499 locations in our State and they see a line, one of the ways we try to reduce that is by introducing electronic poll books.

Now, Madam Chairperson, I really want to revisit that question about standardization.

Ms. FUDGE. Okay, but this is my time. I am trying to get answers to my questions.

Mr. MERRILL. I just want to make sure she knows.

Ms. FUDGE. Okay. Just hold one second for me.

Mr. MERRILL. Yes, ma'am.

Ms. FUDGE. Ms. Schneider, you talked about the cost of trying to assist States. What do you think it would cost to have a fair election in every State in the country because they have machines that are not going to be easily hacked, that they have a paper trail? What does that cost?

Ms. SCHNEIDER. Well, I think that there have been published estimates of the cost, but in the Secure Election Act from last session, and in the security part of the H.R. 1, the $1.2 billion that is allocated for this purpose is a good start. We know—I can speak specifically for Pennsylvania where 83 percent of the counties in Pennsylvania had unverifiable and vulnerable systems, and the estimate for just Pennsylvania was close to $100 million to replace just those systems. So, I think that the first thing is an influx of investment right now, and then sustainable funding going forward.

Ms. FUDGE. All I can say is that I am more concerned now than when you came in about how easily our systems are compromised, and the fact that States don't have the resources to ensure to every one of their citizens that their vote is going to count. Thank you so much, all of you.

Mrs. DAVIS of California. Thank you.

Mr. Raskin.

Mr. RASKIN. Thank you, Madam Chairperson. Thanks to the witnesses. It seems as if the cyber age has made political democracy more vulnerable, and our elections more susceptible to attack and manipulation. We know from the Mueller report that there was a sweeping and systematic campaign by Russian operatives to destabilize and change the course of the American election.

One part of it was pumping ideological poison into the American body politic through Facebook and Twitter and other social media. Another part was the cyber espionage of the DNC, the DCCC, and the Clinton campaign in order to release emails into the election. And the third part of it was the direct efforts to hack into State election systems.

We also know from the intelligence community today that the same bad actors have not gone away and are planning a return engagement with the American people in 2020. And there might be other bad actors now who have decided to enter the sport, given the spotty defenses and response of the American Government. The good news, I think, is that there is a good deal of expert consensus as to what needs to be done to better secure our elections, and I just want to see if all of you all agree with these points.

The first is that we should get rid of paperless voting machines and move to voting systems with voter marked paper ballots. Is that something that there is consensus on? Okay. It looks—let the record show I think everybody is nodding their heads.

Secondly, we need to update and replace out-of-date computer software in States that are still using antiquated and obsolescent systems. Everybody agrees with that, yes?

Ms. BENSON. Yes, but we need to do so in way that carries a sustainable funding source because updating it now means it will be out of date in five years.

Mr. RASKIN. Good. That is a strong point. We have got to be thinking long term, not short term, in terms of all of these remedies.

We need to adopt post-election audits in order to determine whether there are strange things going on. Does everybody agree with that? Yes. And then the Federal Government ought to provide greater cybersecurity resources to help thousands of different electoral jurisdictions across the country fortify their cyber defenses and defend the integrity of our elections. Does that sound right to everybody?

Okay. So how would we characterize where the States are in terms of developing their responses in order to be ready and secure for the 2020 elections? Is there somebody who would be willing to state where they think that the State elections are, the systems are? Ms. Benson.

Ms. BENSON. I will start.

Mr. RASKIN. Please.

Ms. BENSON. I think that a partnership, a strong partnership with State and local officials and the Federal Government is key, and frankly, the Federal Government has both the leadership, a standard establishing role, and an educational role to play for many State and local officials who come to the jobs, perhaps new to the area, and could benefit significantly from ongoing educational awareness and training to the point where if there is a problem identified, you are not simply telling us the problem, you are providing us with the tools, resources, and education to fix it.

Mr. RASKIN. And in some sense, America's problems are unique here, because we have such a decentralized system of electoral administration. In most countries, certainly our neighbors, Mexico and Canada and the European countries, there are national elec-

toral commissions. I think in Mexico, there is even like a national electoral supreme court. But there are national electoral commissions whose sole job, as professional nonpartisan entities, is to administer elections fairly. And we don't have anything like that, right? We have got the Federal Election Commission whose sole jurisdiction is campaign finance and is almost completely dysfunctional even with respect to that. We don't have a national electoral administration, so we depend on the States and the counties and the cities to do it, right?

Mr. MERRILL. Congressman, if we did not allow that to happen the way that it is, according to the 10th Amendment, so those decisions are best made at the local level, at the State level. It would be a lot easier to infiltrate the system and to prepare it to be compromised.

Mr. RASKIN. You think it is easier to defend 8,000 different systems than one system?

Mr. MERRILL. I think it is easier to defend an individual State system than it is if you just knew that on one particular day, using one set of equipment that is used in the entire Nation——

Mr. RASKIN. But can you imagine if America's military defense was provided by the 51 different jurisdictions.

Mr. MERRILL. Yes, sir, but we are not talking about the defense.

Mr. RASKIN. It is an analogy, yes.

Mr. MERRILL. Well, but it is not an accurate one, in my estimation, based on what we are trying to do. That is why I think we need to make sure that equipment is approved, equipment is evaluated, and equipment is documented and recorded as to its effectiveness in election administration.

Mr. RASKIN. Okay. I yield back. Thank you.

Mrs. DAVIS of California. Thank you both. We are going to do another round here quickly, so I want to turn to the Ranking Member, Mr. Davis.

Mr. DAVIS of Illinois. I know everybody is excited for the second round, right?

Mr. Merrill, you were making a point earlier and were not able to finish that point. I would like to give you some time to do that if you want.

Mr. MERRILL. Well, there are a couple of things, Congressman. One of the things I think it is important to note, the gentlelady from Ohio, who has since had to be excused, I think it is important to note that according to all reports that we received from Homeland Security, from counterintelligence, from the Central Intelligence Agency, from the FBI, there was never an incident or occurrence in any of the 50 States in the Union where tabulation changes occurred during the 2016 election. I think that is very important to note.

It is very important to recognize that fact, that the Russians did, indeed, infiltrate our systems, but primarily through social media, and through influencing people in their decision making. When it comes to the administration of the elections, no votes were changed. No equipment was touched. There have been no changes occur to the votes that were cast for those candidates.

The other thing that I wanted to talk about, Congressman, in relation to election equipment. What we could really benefit from in

Alabama, in Michigan, in all other States in the Union is to have a centralized effort to evaluate the effectiveness of election equipment, whether it be for voter registration purposes, whether it be for voter administration purposes, electronic poll books.

And as a member of the Election Assistance Commission Standards Board, one of the things I have advocated for is that we need to have the EAC be a central repository where they could evaluate the effectiveness of equipment. And if they noted failures, or failures were recorded, they could come back and say in a report, much like Consumer Reports used to do for all of us that are old enough to remember it where they don't recognize, or recommend, that a specific vendor be selected, but they say this is what we know about the successes. This is what we know about the failures. And in doing so, it puts us in a better position when we are trying to determine if this is a specific group we need to do business with, or a product that we need to purchase.

Mr. DAVIS of Illinois. All right. Well, I agree with your earlier statement. Facts matter, statistics matter and help us determine how we effectively spend taxpayer dollars to ensure that we have the fairest, safest, most secure election systems.

Secretary Merrill, you worked with DHS going up into the 2018 elections, right?

Mr. MERRILL. Yes, sir, and still do today.

Mr. DAVIS of Illinois. What were your thoughts initially about DHS coming in and helping?

Mr. MERRILL. I was a little bit irritated. Part of it was because when we were told by Secretary Johnson before the elections in 2016 that the Department of Homeland Security was going to take over the elections process, that is a real concern, because that is not an area that those individuals have been trained to take over and to help us be able to effectively administer the elections. What we need is support, and we need assistance, and when possible, funding to assist us in that area.

But for the Federal Government to come over and to overreach and to take over the administration of the elections at all levels, first, I don't think it is appropriate. Secondly, I don't think it is constitutional.

Mr. DAVIS of Illinois. So that was your worry in 2016?

Mr. MERRILL. Yes, sir.

Mr. DAVIS. But right now, what are your thoughts about 2018?

Mr. MERRILL. Yes, sir. It has continued to improve, because one of the things that we have seen is, they have wanted to work with us, and we made our position known to Secretary Johnson and through the Obama administration, and then to President Trump and through Secretary Nielsen. We have found them to be very receptive to our request. I have had, in the last 15 months, two private meetings with Secretary Nielsen and with other team members. We have visited with her and other people in Homeland Security to talk about the issues that have been so important and so relevant to us. They have been very receptive, very responsive. They have offered assistance. They have offered assistance at the State and local level in Alabama. I know they have done that in other States as well.

Mr. DAVIS of Illinois. They haven't come in and required you to do things?

Mr. MERRILL. No, sir. They said that we are available. If you would like to enter into an agreement with us, we would be supportive, but not what we would consider overreach where they come in to take over the system.

Mr. DAVIS of Illinois. How many of your colleagues that are secretaries of state, or in my State of Illinois, it would be the State Board of Elections. How many do you think would be receptive to mandatory Federal assistance?

Mr. MERRILL. Not very many. I think there is some that would be interested in having a stronger partnership than we have if they could get certain benefits from it. But we think, and when I say "we," I am talking about the colleagues that I am the closest to. Much like Thomas Jefferson suggested that that government which governs best governs least. That is the sum of good government.

Mr. DAVIS of Illinois. Well, Mr. Secretary, thanks for your response. I have no idea why my red light speeds up faster than everyone else's, but it always happens that way, so I yield back.

Mrs. DAVIS of California. Thank you. I will recognize myself for five minutes and just follow up with this discussion a little bit, because, you know, it is possible to think about a time when a jurisdiction, when the State doesn't have proper cybersecurity systems, and in that case, what are we looking at? Should there be a role for the Federal Government to make sure that their system is not as vulnerable to hacking as perhaps a neighboring State?

Mr. MERRILL. Yes, ma'am. And one of the things that I would suggest that, much like the appropriation that we just received from the EAC, if there were certain expectations about the way that a block grant of resources could be received by the State and be utilized by that State in certain areas to make sure that certain purchases were being made, or certain systems were being implemented to prevent vulnerabilities or to keep certain vulnerabilities from being exposed, that would be very helpful to us.

But for certain things to be introduced, as it was in H.R. 1, to say that you must have these things in place, you must do these and have an unfunded mandate, that is not good for any State, no matter whether you have a great deal of resources in your statement or you are limited with your resources.

Mrs. DAVIS of California. So it sounds like you are talking about some enforcement capability in some areas, but not in others.

Anybody else want to comment on that quickly?

Ms. BENSON. Yes. I would like to offer the alternative perspective. With all due respect to my good friend, Secretary Merrill, I am coming at this as a long-time academic and voting rights scholar. I feel very strongly that there is a leadership role for the Federal Government to play. It is in partnership and in collaboration with the State and local governments, as I have said repeatedly today, but the Federal Government cannot, and should not, abdicate its role as it has historically to set the standards and expectations that all States must meet.

I think it is the basic Constitutional imperative of equal protection, and it takes into consideration that while every State does have unique challenges, there are some standards of expectations

that, especially if we are receiving Federal funding, I think many of us, myself included, would be comfortable working with the Federal Government in seeking to meet. It is a dance to determine how deep and specific those standards should be, and I acknowledge that, but I don't think that is a reason to not have basic data-driven, fact-based solutions, and bars that States should strive to meet if they are receiving Federal assistance.

Mr. DAVIS. Thank you. Yes, please.

Ms. SCHNEIDER. I just wanted to share with you my experience in 2016 with the Department of Homeland Security. At that time, they offered their services free of charge to State and local jurisdictions who wished to receive them, and we were able to engage with the Department of Homeland Security to run a penetration test and assessment of our networks before the 2016 election, which we were very grateful for, and we think that that is the kind of partnership that should occur, and I think that they need adequate resources to offer those services to every jurisdiction who would like them.

And to your earlier question before about whether you get notification, there is the multi-State information sharing association from the Center for Internet Security, that it does go to the State CIOs, but we did receive that in Pennsylvania, and if it was unclassified, it was filtered down, and also, through the Pennsylvania Emergency Management Association.

Mrs. DAVIS of California. Okay. Thank you very much. And that was in real time, you are suggesting. Was it a week from the occurrence, or right away?

Ms. SCHNEIDER. No. If they were unclassified, they were right as they occurred.

Mrs. DAVIS of California. Okay. Great. Thank you.

I wonder if you could, just for a moment, think about whether you believe that there is anything that voters should be doing to make our systems more secure? Is there an educational piece that we have not addressed in this country?

Ms. SCHNEIDER. There is one thing that voters could do right before or at any point in the election cycle, is to check their registration, and make sure that their information is correct, their address is correct, their polling place is correct, because if there has been an attack or tampering in the registration system, you can detect it and correct it in advance.

Mr. HALL. And I would say check your ballot to make sure that the thing you cast reflects your intent and volunteer to be a poll worker. This is a vast volunteer force, and it is the pinnacle, I think, of civic duty, you know, spending 16 hours counting your fellow citizens' votes.

Mrs. DAVIS of California. Thank you. And that is particularly in areas where there is a very diverse community, we need to have people come forward who understand language and culture and a whole host of other things. Thank you very much. I appreciate all of you for being here, and I am going to turn to Mr.——

Mr. MERRILL. Madam Chairperson, if I may add to that in response to your question. One of the things we have done is try to encourage non-voters to become poll workers. We are passing legislation now in Alabama, it has already passed both chambers, to

allow 16- and 17-year-olds to be able to work the polls which can increase civic responsibility.

Mrs. DAVIS of California. Thank you. Appreciate that as well.

Mr. Loudermilk, do you have an extra question?

Mr. LOUDERMILK. Thank you, Madam Chairperson. I want to shift away from voting, because I would really love to continue that conversation, and I think Mr. Hall and I could have a good conversation on that. I think we see eye to eye on this.

I want to move over to the cybersecurity aspect of it now, and from my background in cybersecurity, any breach at some, or at least the majority of breaches at some level, have human error involved in it. There is usually some aspect, and a lot of times, it is a failure to act. It is with a patch or it is with something—at Equifax, it was failure to actually have a patch. And Mr. Hall is right. You cannot create a 100 percent secure system.

When I was working in intelligence in the Air Force, we commissioned a vendor to create a completely secure system. They came pretty close. It was very secure, but it was so slow, nobody could use it. So it is always—it is a balance there.

I do want to say something, and Mr. Merrill brought up a good point. It is from my experience of working in IT, it is always more secure to have multiple vendor systems over a single vendor system which if that is compromised, then everybody has—the bad guy has 100 percent access to everything. But you have to have a set of standards that the vendors operate by, and I think that is a role that we can play as a recommended set of standards still leaving the 10th Amendment, the States authority to conduct and operate their elections. But if you are going to use certain types of systems, they should meet these standards. I think that is clear.

But back to the cybersecurity aspect. Is anyone on the panel familiar with OODA loop? OODA. O-O-D-A. A little bit surprised because that is used in cybersecurity. It is a cycle of decision making that you use to defeat an adversary in a fast-paced, multi-faceted environment. It is OODA. It means——

Mr. HALL. Observe something, detect, act?

Mr. LOUDERMILK. It is observe, orient, detect or decide and act. It basically means you are always observant. You are watching to see what is going on which is happening in our cybersecurity realm right now. You orient yourself to what the threat is or multiple threats coming in. You make a decision of what you are going to do to counter that decision, and you act. And these loops are going continually, and it is used today. The NSA uses it. The CIA uses it. It was developed by an actual Air Force Colonel, so you know, give a few kudos to the Air Force there.

Most cyber risk and breaches come from the last aspect of that, a failure to act. It is you orient, you observe, you decide, and in the case of Equifax, they didn't act to put a patch in. When we go to the 2016 election, and I will open this up to anybody, because I am still trying to figure out why we did what we did. I don't know if you are familiar with Michael Daniel. Michael Daniel was the cybersecurity czar in the previous administration.

When the administration was given evidence that the Russians were actively trying to attack our cybersecurity, or our election systems, when it came to the acting, he was given the order by the

National Security Advisor, Susan Rice, to stand down and not do anything. This was testified before the Senate in 2018 by Michael Daniel, that he received the order to not act to counter the Russians' attempts to interfere with our election system. Can anybody answer why, and maybe that would have a failure to act on the part of the Obama administration?

Mr. HALL. The only thing I can think of is concern with ongoing operations that might have revealed something, but, you know, given that democracy hangs in the balance, I am not sure. I don't know enough about the specifics to say one way or the other.

Mr. LOUDERMILK. I think we could have evolved a lot of stuff, resolved a lot of stuff, had there been the act which is a standard process in cybersecurity.

And one last question for you, Mr. Merrill. War Eagle or Roll Tide?

Mr. MERRILL. My friend, look. There is only two words that you can say. Roll Tide.

Mr. LOUDERMILK. All right. Thank you. I yield back.

Mrs. DAVIS of California. Thank you.

Mr. Raskin.

Mr. RASKIN. Thank you, Madam Chairperson.

Ms. Benson, I just want to follow up with you about a point you were making before. First, there are a number of provisions in our Constitution which confer power on Congress and the Federal Government to regulate elections, right?

Ms. BENSON. Yes.

Mr. RASKIN. For example, the Congress has to guarantee to the people of the States a Republican form of government. Also, there is a specific provision which allows Congress to legislate in the electoral field, right? And under the supremacy clause, it clearly is supreme to the States. And as well, there are the enforcement provisions of a number of amendments in the Bill of Rights, and that is how we have made great progress in our country. Certainly, we would not be where we are in terms of voting with all the problems that we have without the Voting Rights Act of 1965, and that was passed under Section 5 of the 14th Amendment, right?

Ms. BENSON. Yes.

Mr. RASKIN. Is there any serious debate about the Congressional role in trying to make sure that everybody's voting rights are vindicated, and everybody's votes are counted?

Ms. BENSON. I think in Section 2 of the 14th Amendment, I think whether it is the Help America Vote Act, the National Voter Registration Act, the Voting Rights Act of 1965, the myriad of other Federal laws that have been enacted since the inception of our democracy, our democracy is better because of the congressional role in enforcing a basic standard of expectations of protections for all of our citizens.

Mr. RASKIN. And to just tease that out for a moment, haven't the greatest threats to people's voting rights started at the local and State level? Obviously, we have got this new threat of global interference with people's voting rights, but traditionally in our country, haven't the greatest threats arisen locally?

Ms. BENSON. History does show us that some of greatest threats have emerged locally, and some of the greatest successes and pro-

tections for voting rights have also emerged locally when States and local governments have gone beyond what the Federal Government has expected as a standard. I want to make that point as well, but, yes, certainly there is a critical role for the Federal Government to play.

Mr. RASKIN. Yes. I mean, the States have certainly led in terms of the expansion of the franchise, and we know lots of States extended women the right to vote, for example, before the 19th Amendment——

Ms. BENSON. And language protections.

Mr. RASKIN [continuing]. Was adopted. And language protections and extending the right to vote to African Americans. And so that is definitely the case, that we have seen a lot of forward movement in the States that lead to national changes. But in the dynamics of Federalism, Congress has played an essential role in securing people's right to vote. And I think given the new cyber threats to voting security, Congress cannot abdicate that role, and Congress should be really in the forefront of trying to assist the States in making sure that we are fortifying our defenses, so there is not an open door for the kinds of activities that we saw in 2016.

Ms. BENSON. It is a critical role for the Federal Government to play. Also, in acknowledging and being a partner with us, and you know, fully funding the Election Assistance Commission and other existing agencies can go a long way in that regard as well.

Mr. RASKIN. Okay. Madam Chairperson, I yield back to you. Thanks so much.

Mrs. DAVIS of California. Thank you very much.

I might just follow up. Fully funding it and providing some authority so that they can do something about it, correct? I think everybody would agree with that.

Ms. BENSON. And I also want to emphasize as you have seen today, the importance of talking to more State and local officials, because I think you will see multiple different perspectives and opinions, and through that, I think you can develop some Federal expectations and standards.

Mrs. DAVIS of California. Thank you very much. I want to thank all of you for your valuable testimony here, for appearing, and for being very helpful. I also want to let you know that members have five legislative days to revise and extend their remarks, and written statements may be made part of the record. If they have questions, we ask you to please respond in writing as soon as possible. I think there is a deadline on that but respond quickly so they can be made part of the record. Thank you very much. If there are no objections, this hearing is adjourned.

[Whereupon, at 4:00 p.m., the Committee was adjourned.]

SUBMISSIONS FOR THE RECORD

Election Security Hearing
Ranking Member Rodney Davis
Closing Statement

Thank you, Madam Chairperson. I'm thankful our Committee has decided to take up the important issue of election security

I know I have little time, but I want to draw the Committee's attention to tools we should be looking at making more widely available in the election realm-such as WHOIS data (Who-is-data) which has proven useful time and again at identifying the entities behind nefarious web sites

Currently some domain name providers are restricting access to such data, and while our Federal agencies are working through diplomatic channels to reinstate access to WHOIS data, it is something we will want to watch closely to ensure we have the tools we need to secure our elections

Securing our elections cannot be a partisan exercise I have always been supportive of enhancing our election security, which is why I introduced an amendment during H R 1 discussions to replace Title III, the Majority's partisan attempt of election security, with the Senate's bipartisan bill, the Secure Elections Act

Again, I think we can all agree on this panel that we have work to do when it comes to ensuring our elections are safe from interference, and I'm willing to work with my colleagues when they are ready to include us in discussions on future legislation.

○